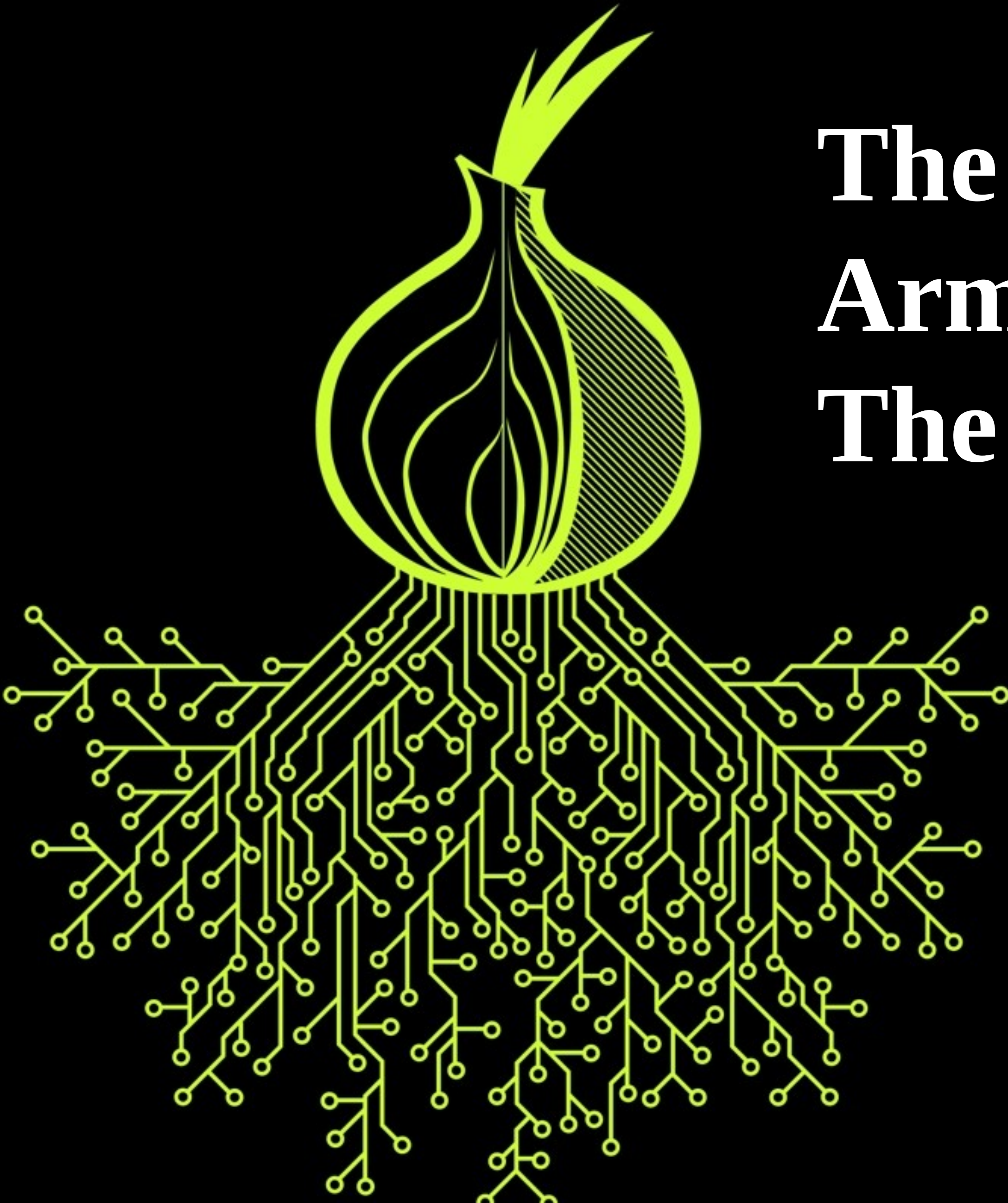


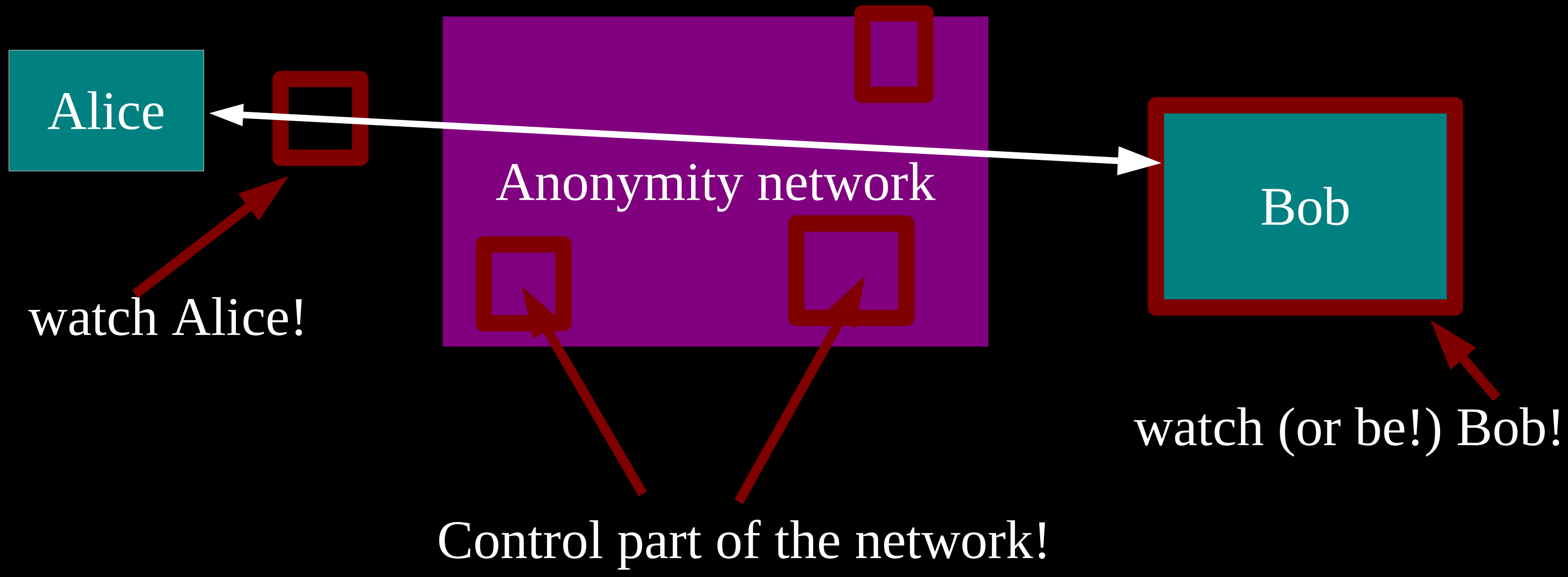
The Tor Censorship Arms Race: The Next Chapter



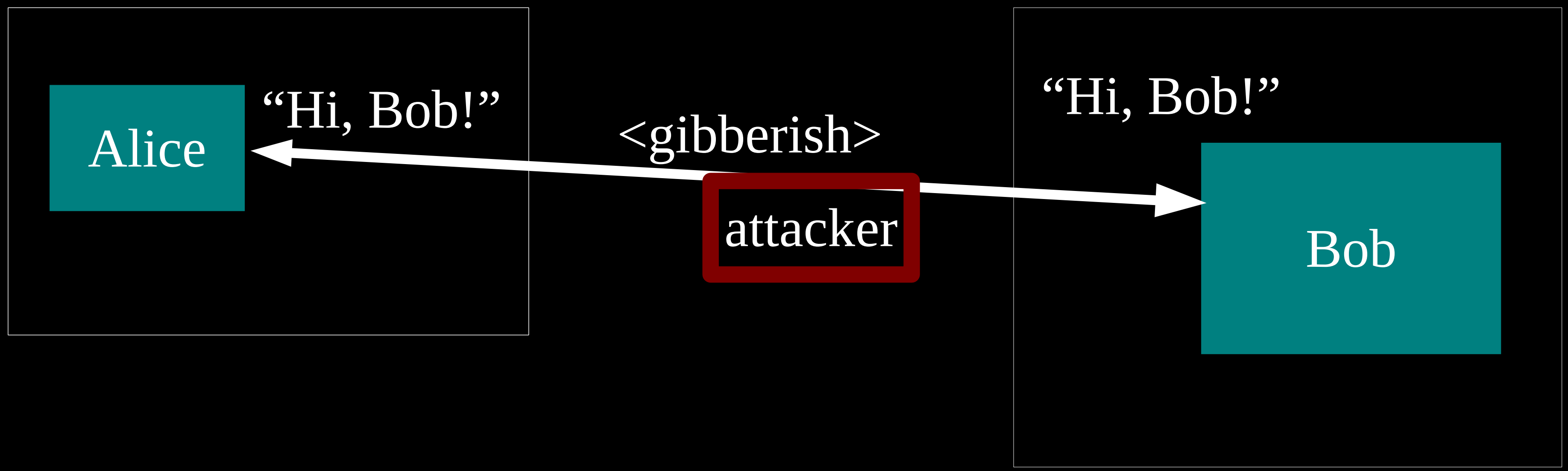
- Online Anonymity
  - Open Source
  - Open Network
- Community of researchers, developers, users and relay operators.
- U.S. 501(c)(3) non-profit organization


Estimated 2,000,000 to 8,000,000
daily Tor users

Threat model: what can the attacker do?



Anonymity isn't encryption: Encryption just protects contents.



Metadata

Data about data

"Metadata was traditionally in the card catalogs of libraries"

-- Wikipedia



"We kill people based on metadata"

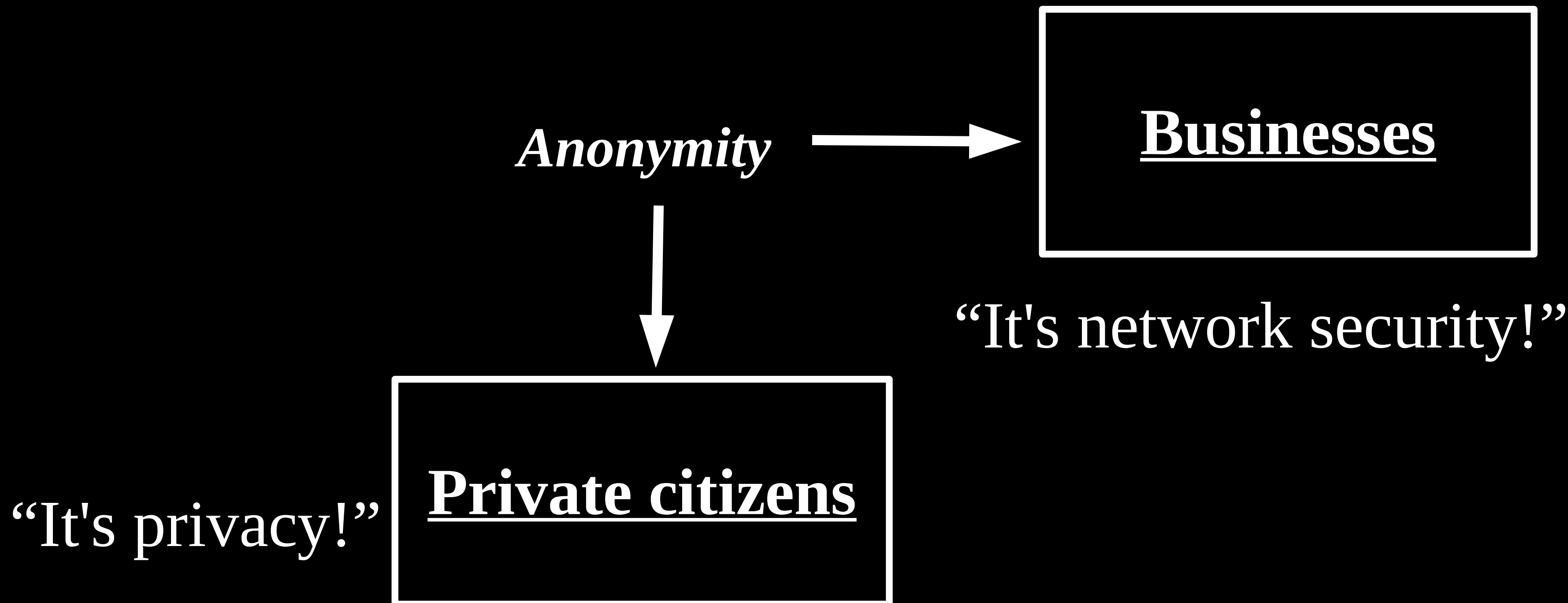
Anonymity serves different interests for different user groups.

Anonymity

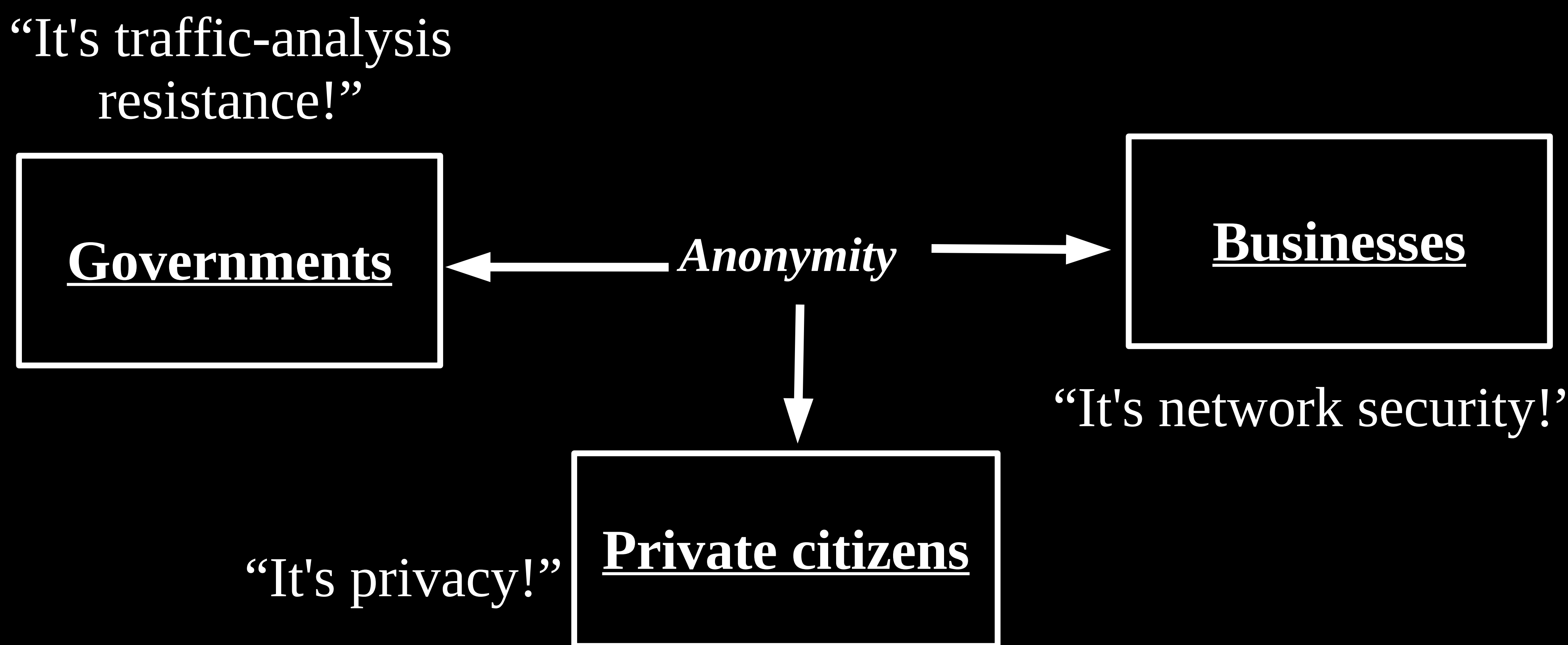
<u>Private citizens</u>

“It's privacy!”

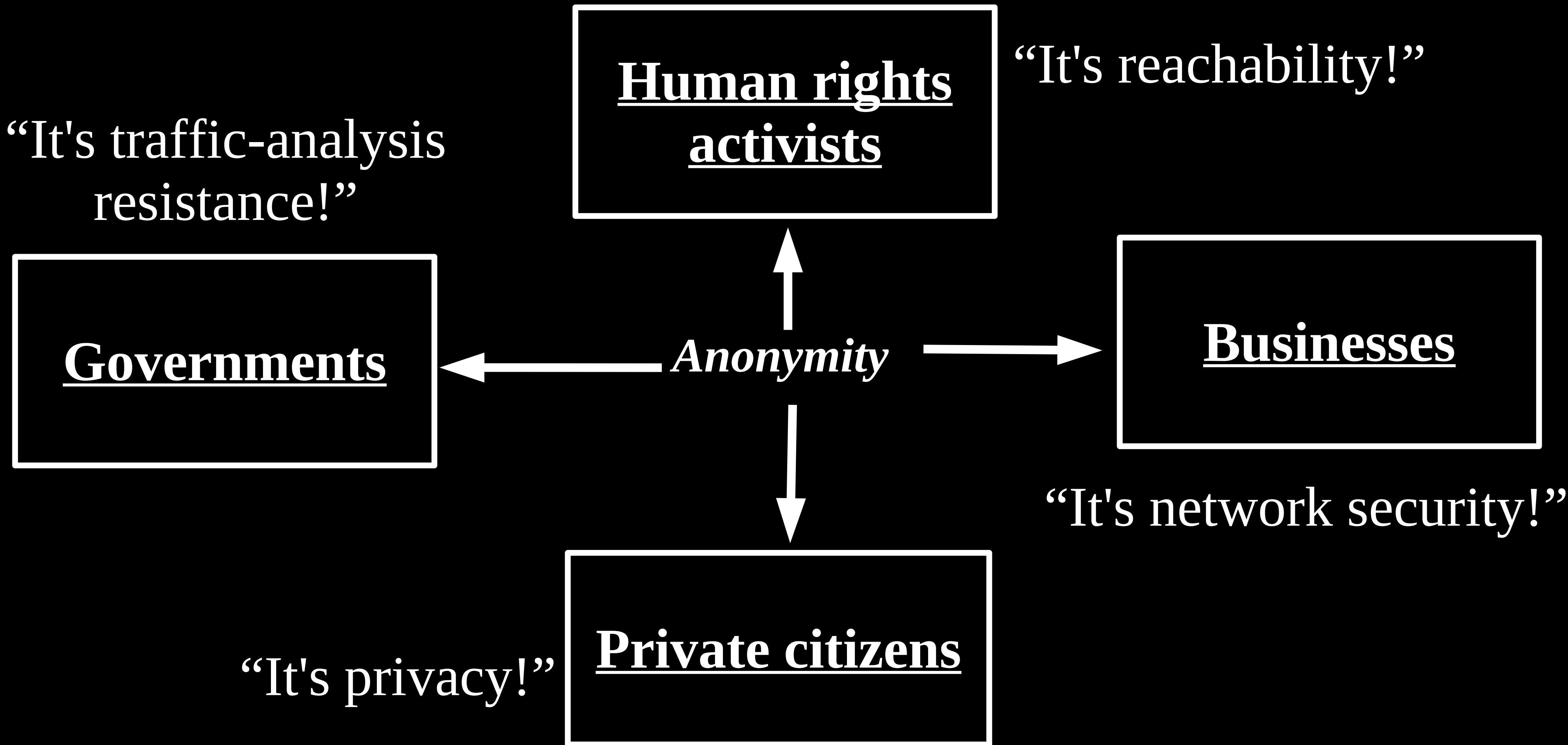
Anonymity serves different interests for different user groups.

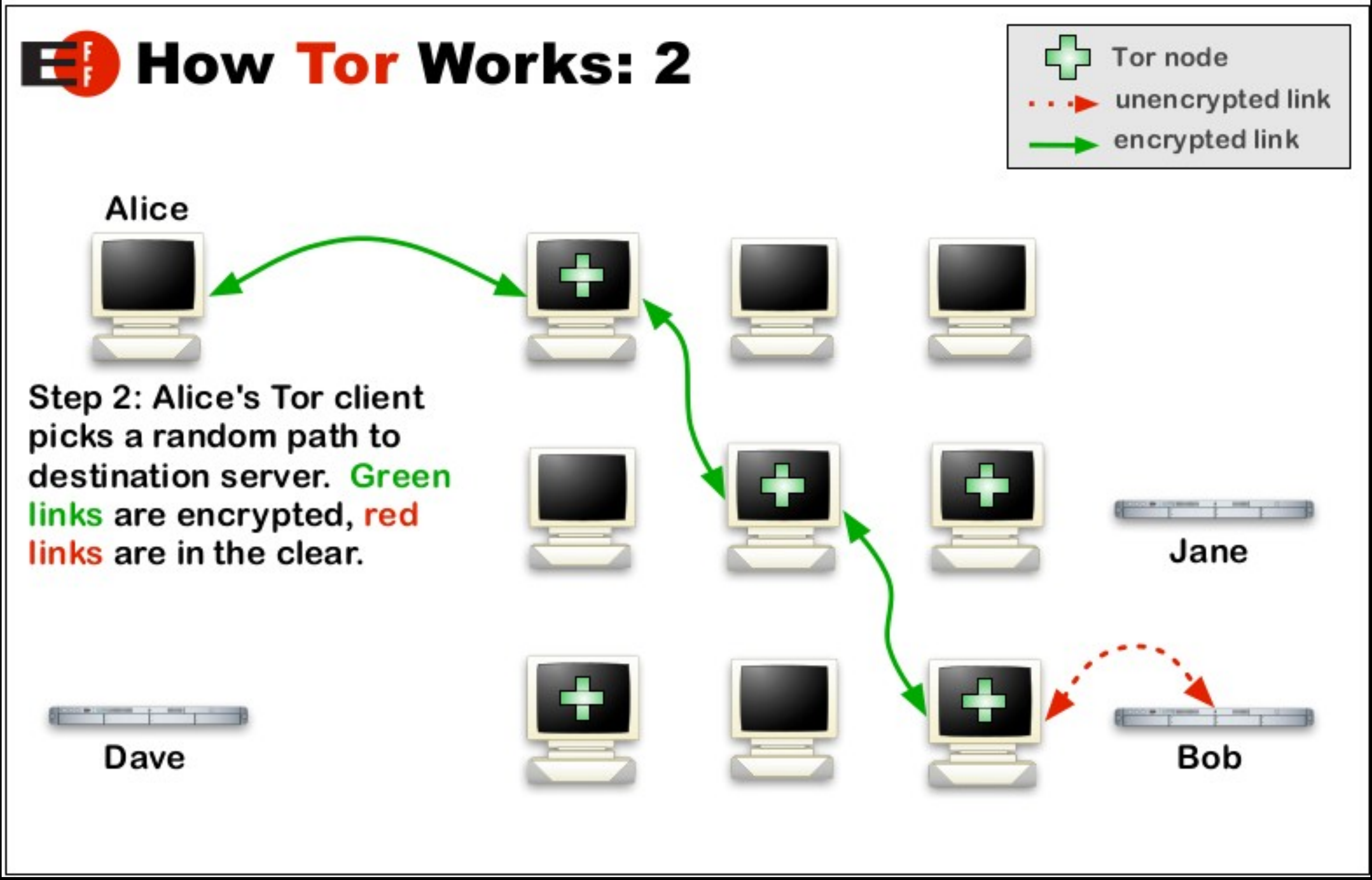


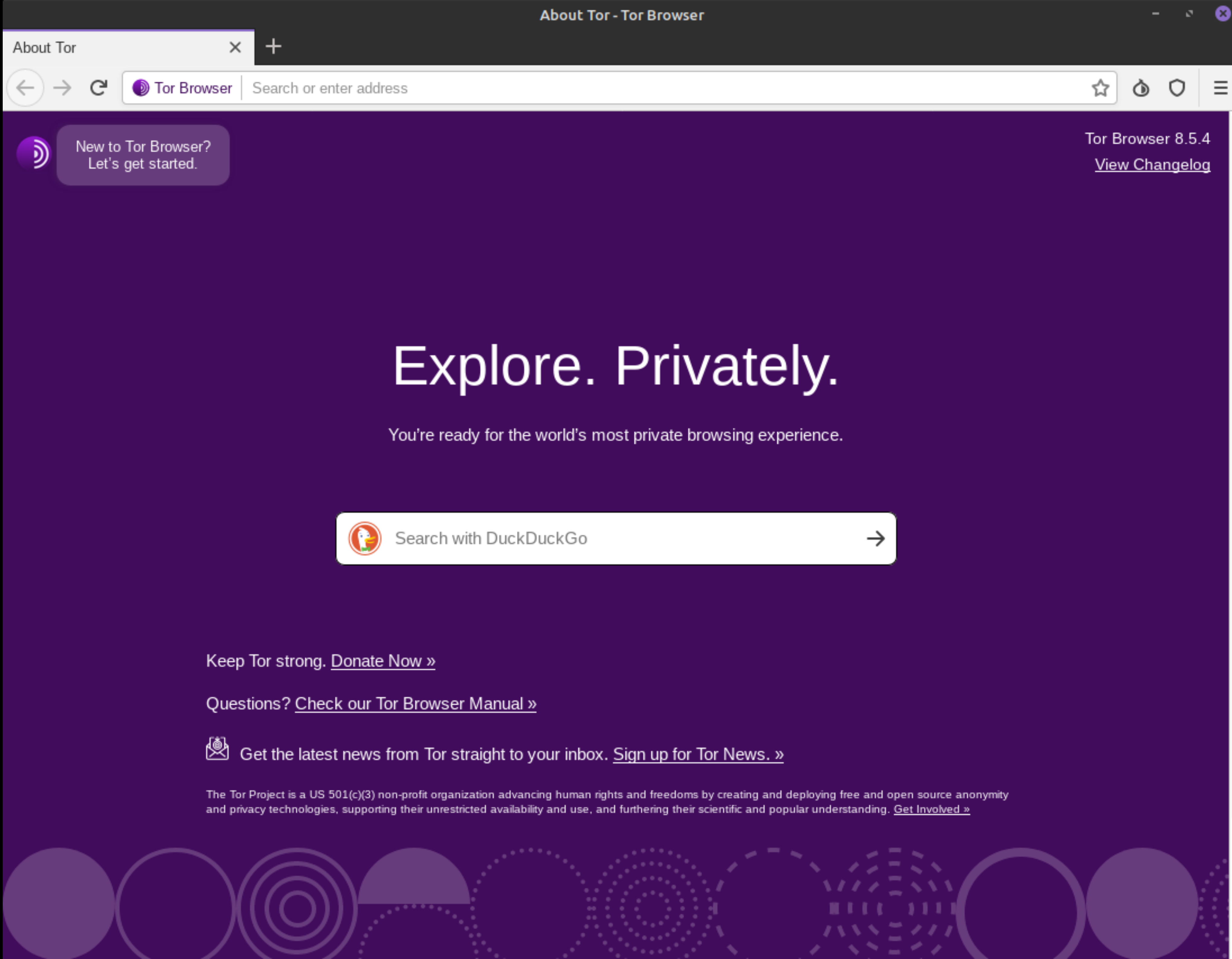
Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.

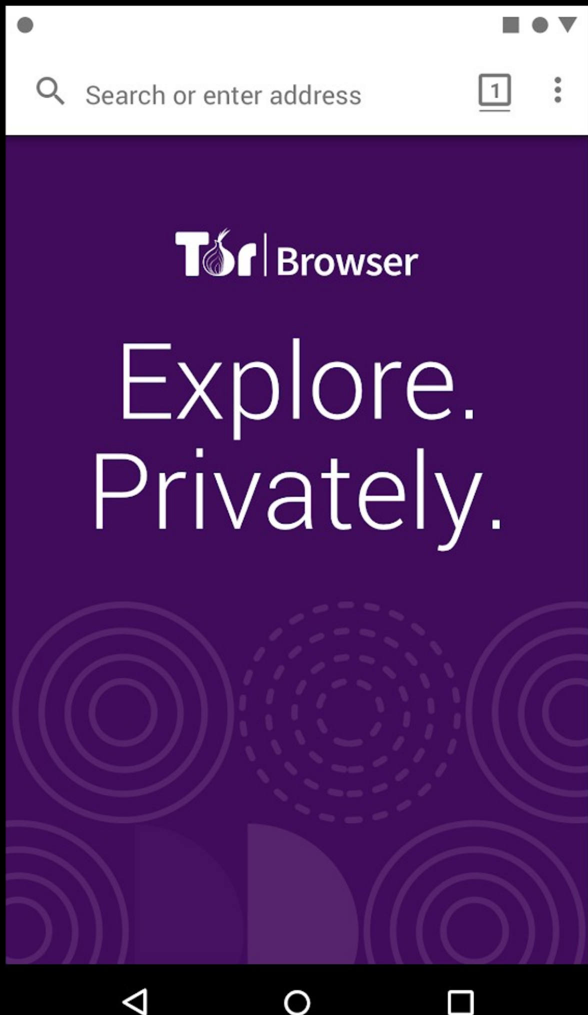


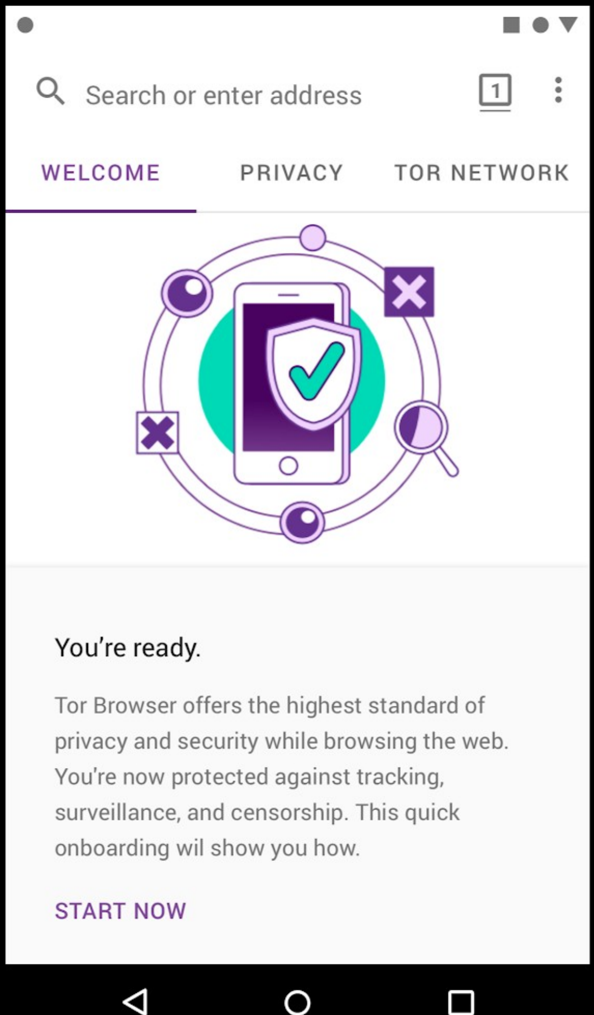

How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

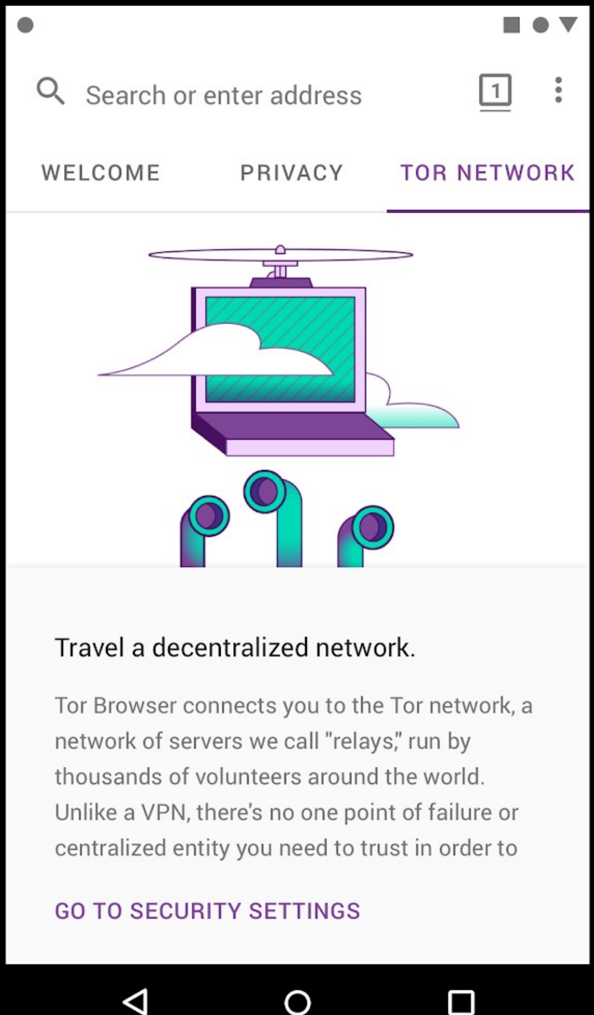

About Tor - Tor Browser
About Tor
Tor Browser
Search or enter address
New to Tor Browser?
Let's get started.
Tor Browser 8.5.4
View Changelog
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Keep Tor strong. Donate Now »
Questions? Check our Tor Browser Manual »
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

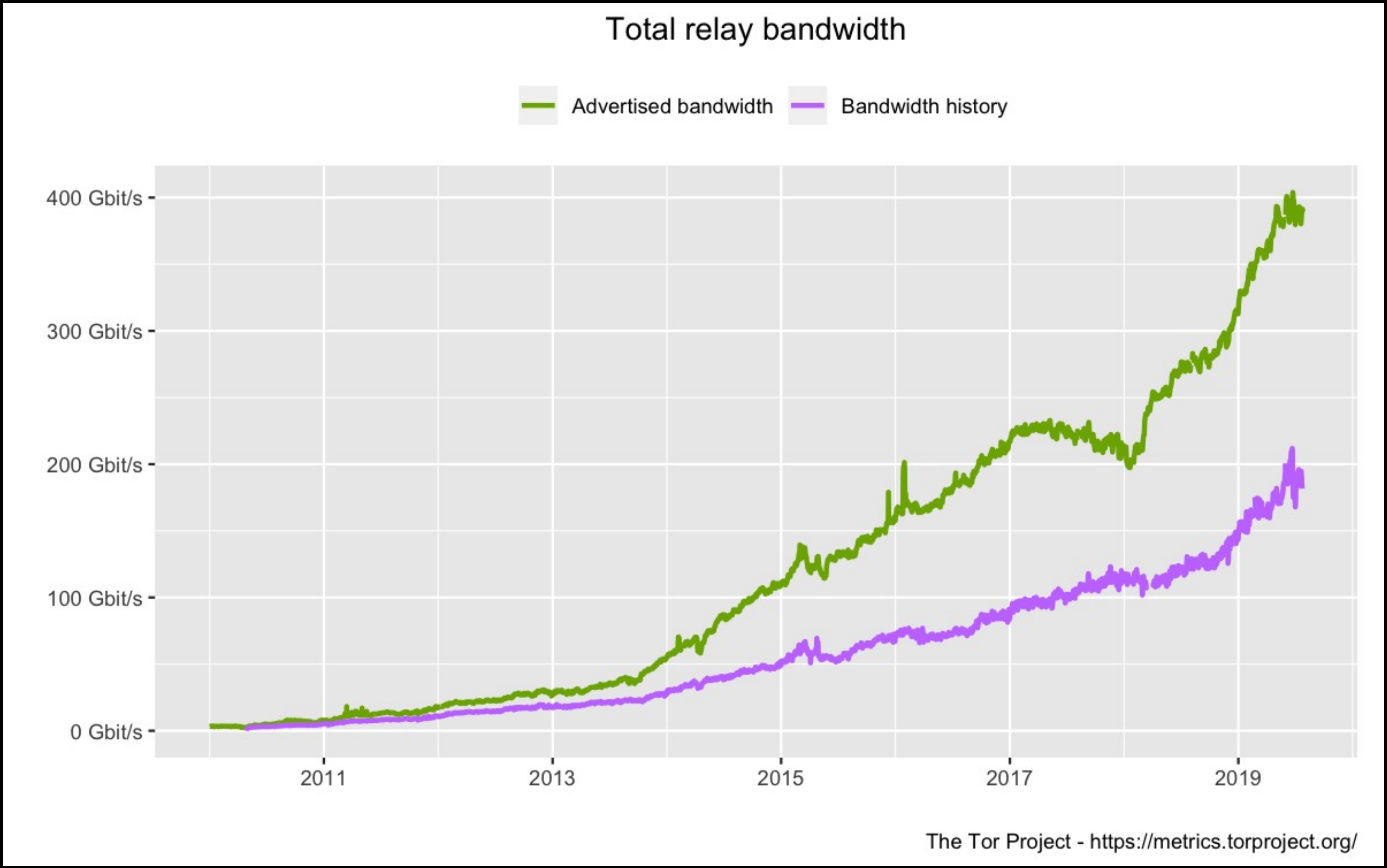
Tails

the**amnesic**incognito**live**system


Search or enter address
Tor Browser
Explore.
Privately.


Search or enter address
WELCOME
PRIVACY
TOR NETWORK
You're ready.
Tor Browser offers the highest standard of privacy and security while browsing the web. You're now protected against tracking, surveillance, and censorship. This quick onboarding wil show you how.
START NOW


Search or enter address
WELCOME
PRIVACY
TOR NETWORK
Travel a decentralized network.
Tor Browser connects you to the Tor network, a network of servers we call "relays," run by thousands of volunteers around the world. Unlike a VPN, there's no one point of failure or centralized entity you need to trust in order to
GO TO SECURITY SETTINGS



Total relay bandwidth
Advertised bandwidth
Bandwidth history
400 Gbit/s
300 Gbit/s
200 Gbit/s
100 Gbit/s
0 Gbit/s
2011
2013
2015
2017
2019
The Tor Project - https://metrics.torproject.org/

Tor's safety comes from diversity

- #1: Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)
- #2: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.

Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction:
  privacy is about choice!

Tor censorship epochs

- Background / Phase 1 (2006-2011):
  Bridges, pluggable transports
- Phase 2 (2011-2019):
  Active probing, obfsproxy, domain fronting, many more countries
- Phase 3 (2019-?):
  Snowflake, obfs4, decoy routing, ...

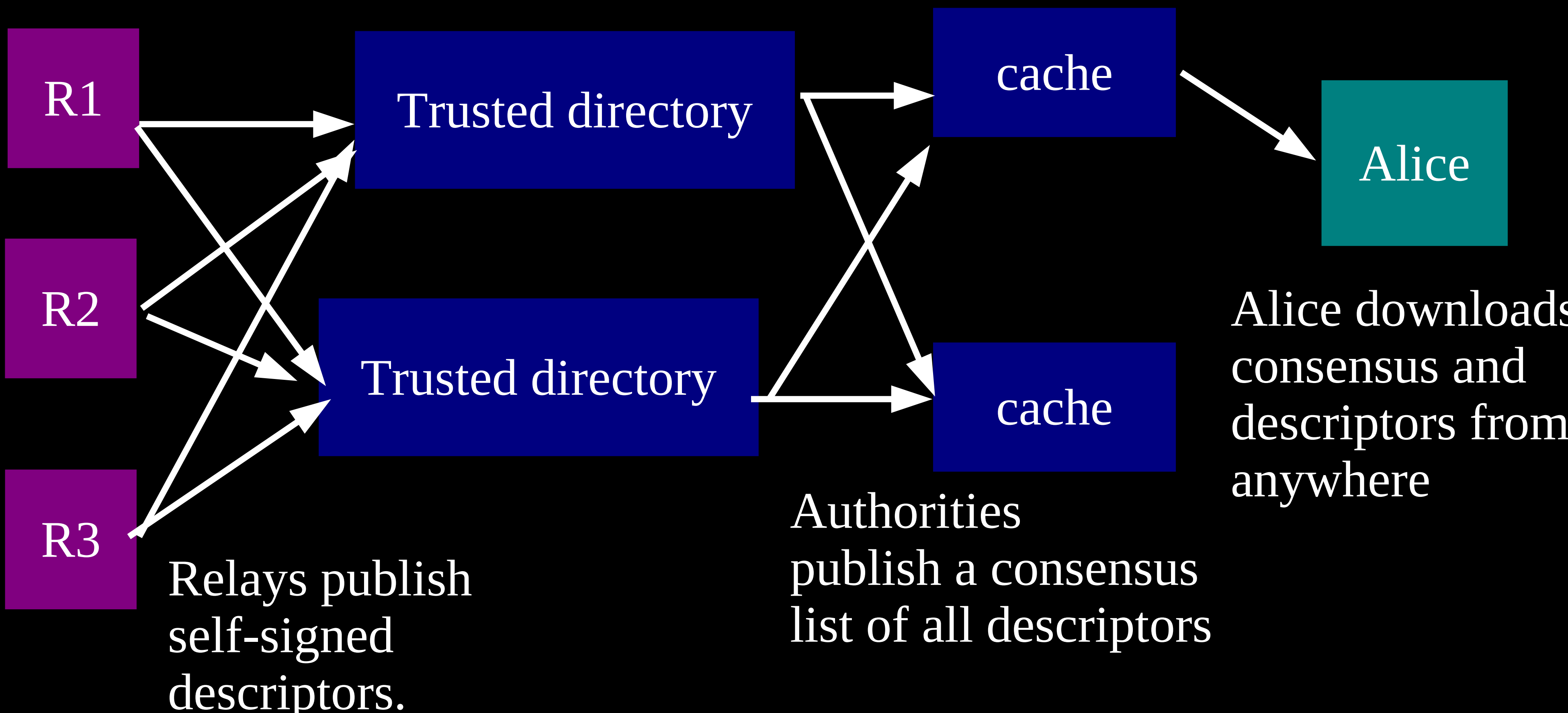
Relay versus Discovery

There are two pieces to all these "proxying" schemes:

a **relay** component: building circuits, sending traffic over them, getting the crypto right

a **discovery** component: learning what relays are available

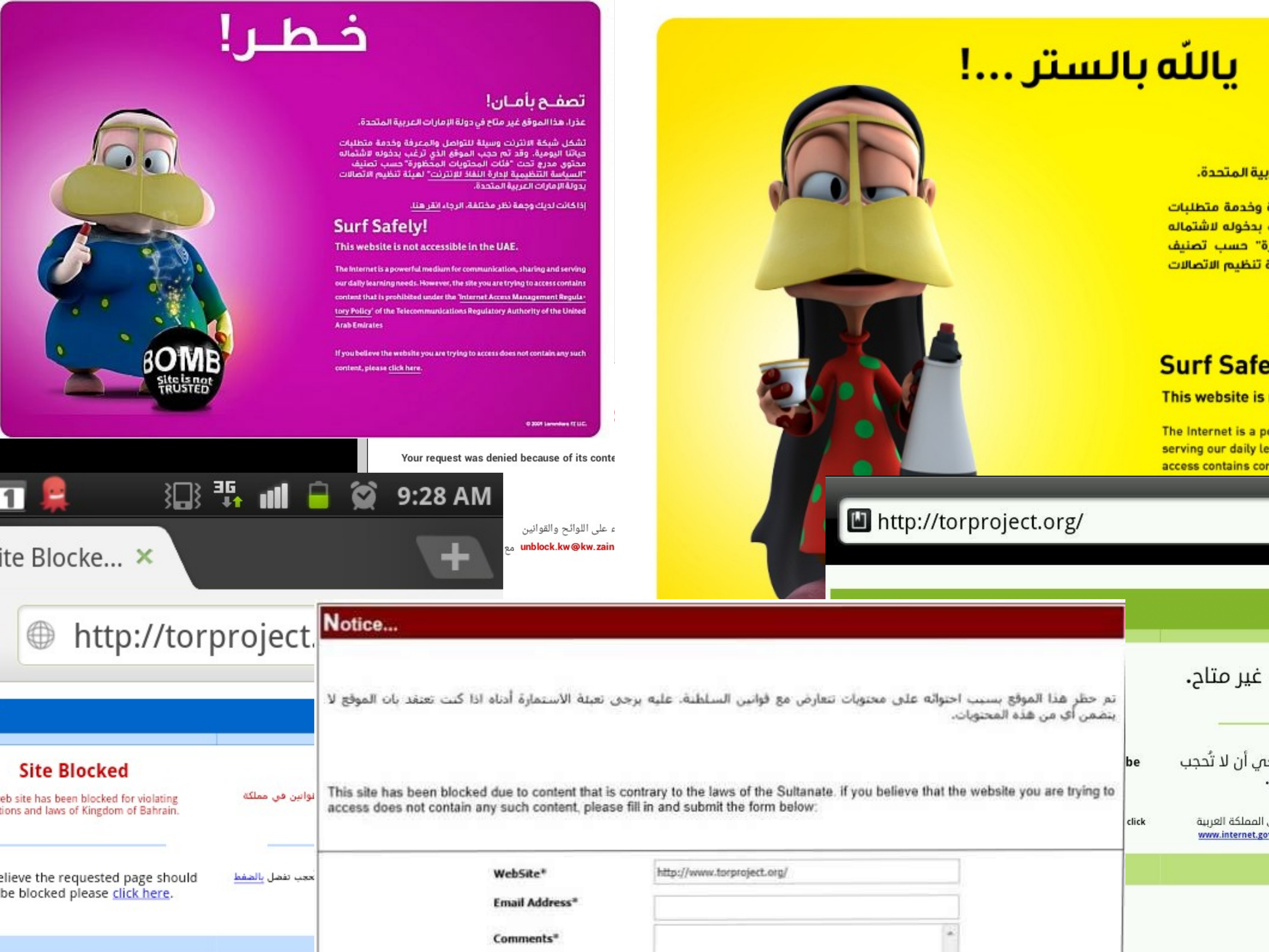
The basic Tor design uses a simple centralized directory protocol.



Early blocking

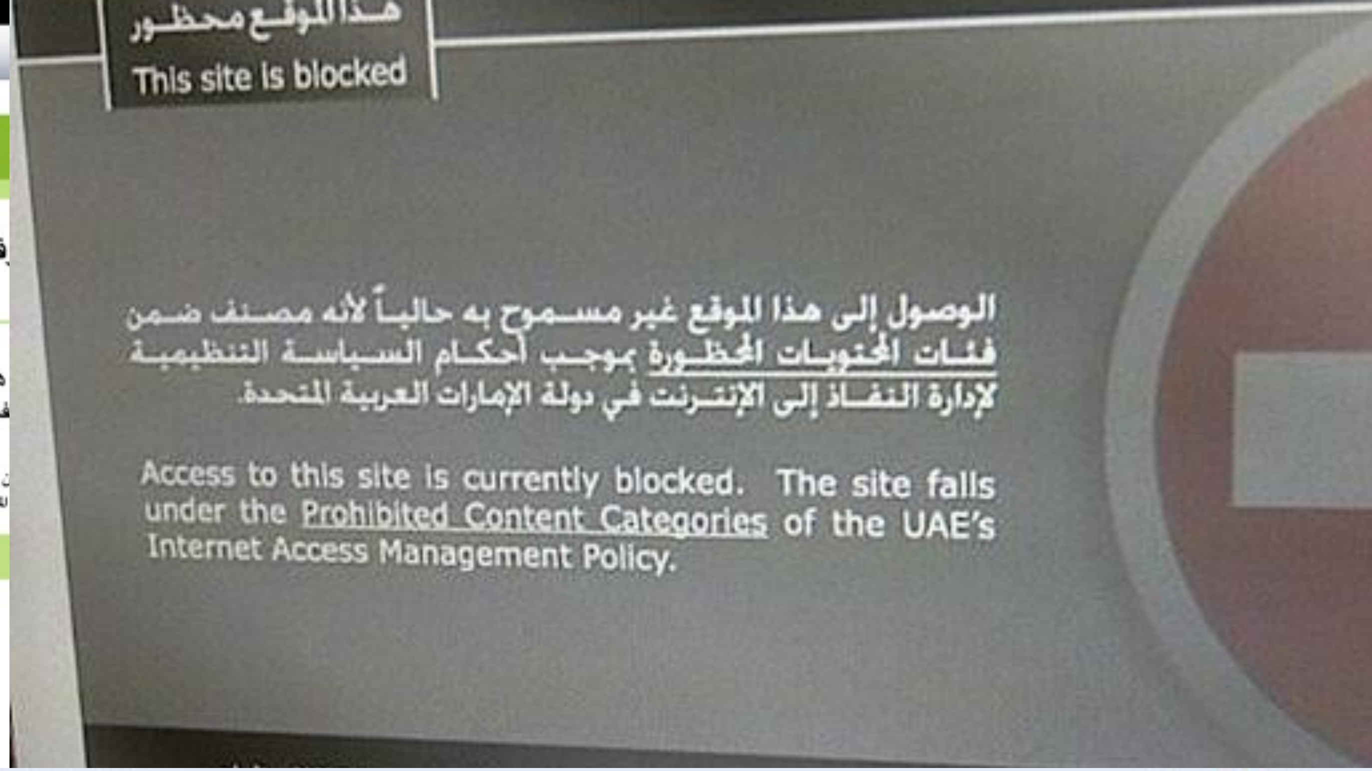
- 2006: Thailand blocks our website by DNS
- 2007: Iran/Saudi Arabia/others use websense/smartfilter to block Tor's http directory fetches.

  The fix: put everything inside TLS.



خطـر!
تصفـح بأمـان!
عذرا، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.
تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.
إذا كانت لديك وجهة نظر مختلفة، الرجاء انقر هنا.
Surf Safely!
This website is not accessible in the UAE.
The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the 'Internet Access Management Regulatory Policy' of the Telecommunications Regulatory Authority of the United Arab Emirates
If you believe the website you are trying to access does not contain any such content, please click here.
BOMB
Site is not TRUSTED
يالله بالستر ...!
Surf Safe
This website is
Your request was denied because of its conte
unblock.kw@kw.zain
9:28 AM
ite Blocke...
http://torproject.
http://torproject.org/
Site Blocked
eb site has been blocked for violating
tions and laws of Kingdom of Bahrain.
elieve the requested page should
be blocked please click here.
Notice...
تم حظر هذا الموقع بسبب احتوائه على محتويات تتعارض مع قوانين السلطنة. عليه يرجى تعبئة الاستمارة أدناه اذا كنت تعتقد بان الموقع لا يتضمن أي من هذه المحتويات.
This site has been blocked due to content that is contrary to the laws of the Sultanate. If you believe that the website you are trying to access does not contain any such content, please fill in and submit the form below:
WebSite*
http://www.torproject.org/
Email Address*
Comments*
غير متاح.


10:00 AM
Blocked URL
ar User,
Sorry, the requested page is unavailable.
قع المطلوب غير متاح.
you believe the requested page should not be blocked please click here.
هذه الصفحة ينبغي أن لا تُحجب
فضل بالضغط هنا.
r more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa
www.internet.gov.sa


هذا الموقع محظور
This site is blocked
الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن فئات المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النفاذ إلى الإنترنت في دولة الإمارات العربية المتحدة.
Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.


KT WATA... ٩:٢١ ص 87 %
Tweet
Blocked by Mada Com...
mada Mada Communications
ان الموقع الذي تحاول زيارته محجوب
Access to this website is prohibited
SITE BLOCKED
This site is blocked according to the goverment filtering policy.
If you feel this page has been blocked in errors, kindly fill out the form and we will investigate .
Thank You .
Required fields are denoted by (*)
Full Name *
Email *
Blocked URL *
Comments
Submit


oops أفا
لقد تم منع الدخول إلى هذا الموقع
This site has been blocked
تم إيقاف عملية الدخول إلى الموقع الذي تحاول زيارته نظراً لاحتوائه على محتويات محظورة
The web page you are trying to access has been blocked as the content contains prohibited materials
إذا كنت ترى أن هناك خطأ في ذلك .. يرجى إرسال رسالة بريد إلكتروني إلى help@isp.qa
If you feel this is an error then please send

Iran throttles SSL (June 2009)

- We made Tor's TLS handshake look like Firefox+Apache.
- So when Iran freaked out and throttled SSL bandwidth by DPI in summer 2009, they got Tor for free

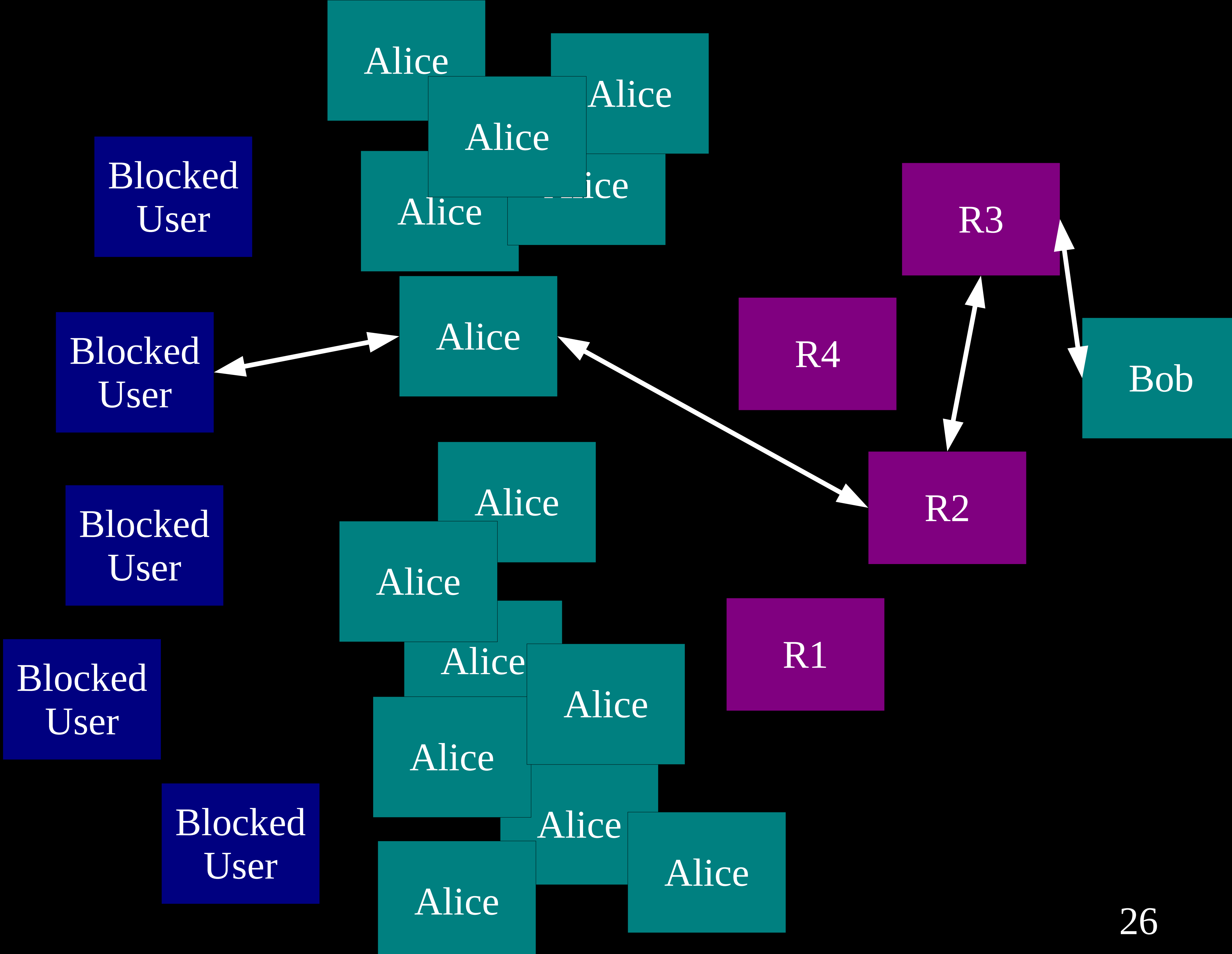
Attackers can block users from connecting to the Tor network

1) By blocking the directory authorities

2) By blocking all the relay IP addresses in the directory, or the addresses of other Tor services

3) By filtering based on Tor's network fingerprint

4) By preventing users from finding the Tor software (usually by blocking website)



Alice
Alice
Alice
Alice
Blocked User
Blocked User
Alice
R3
R4
Bob
R2
Blocked User
Alice
Alice
Alice
Alice
R1
Blocked User
Alice
Alice
Blocked User
Alice
Alice

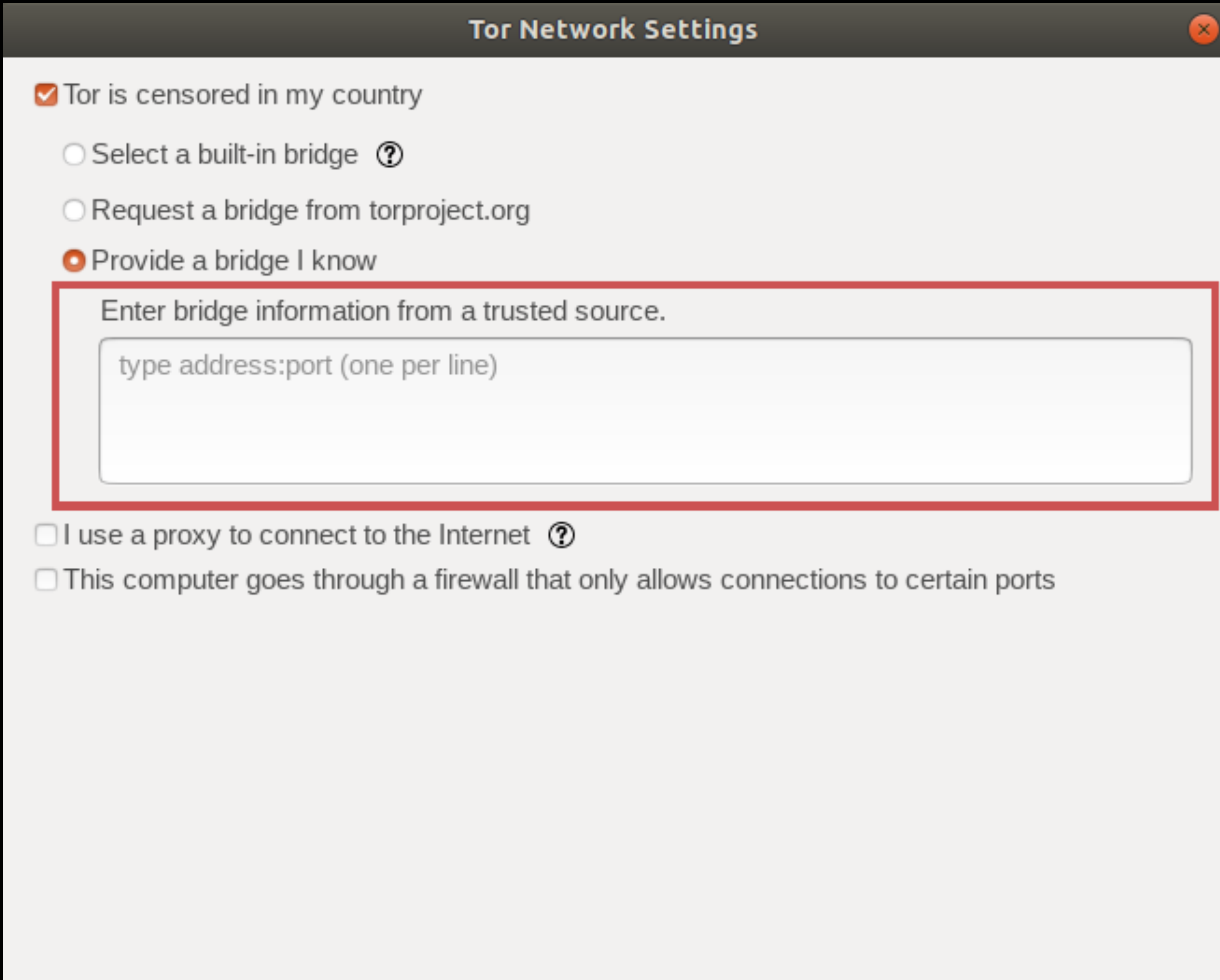
How do you find a bridge?

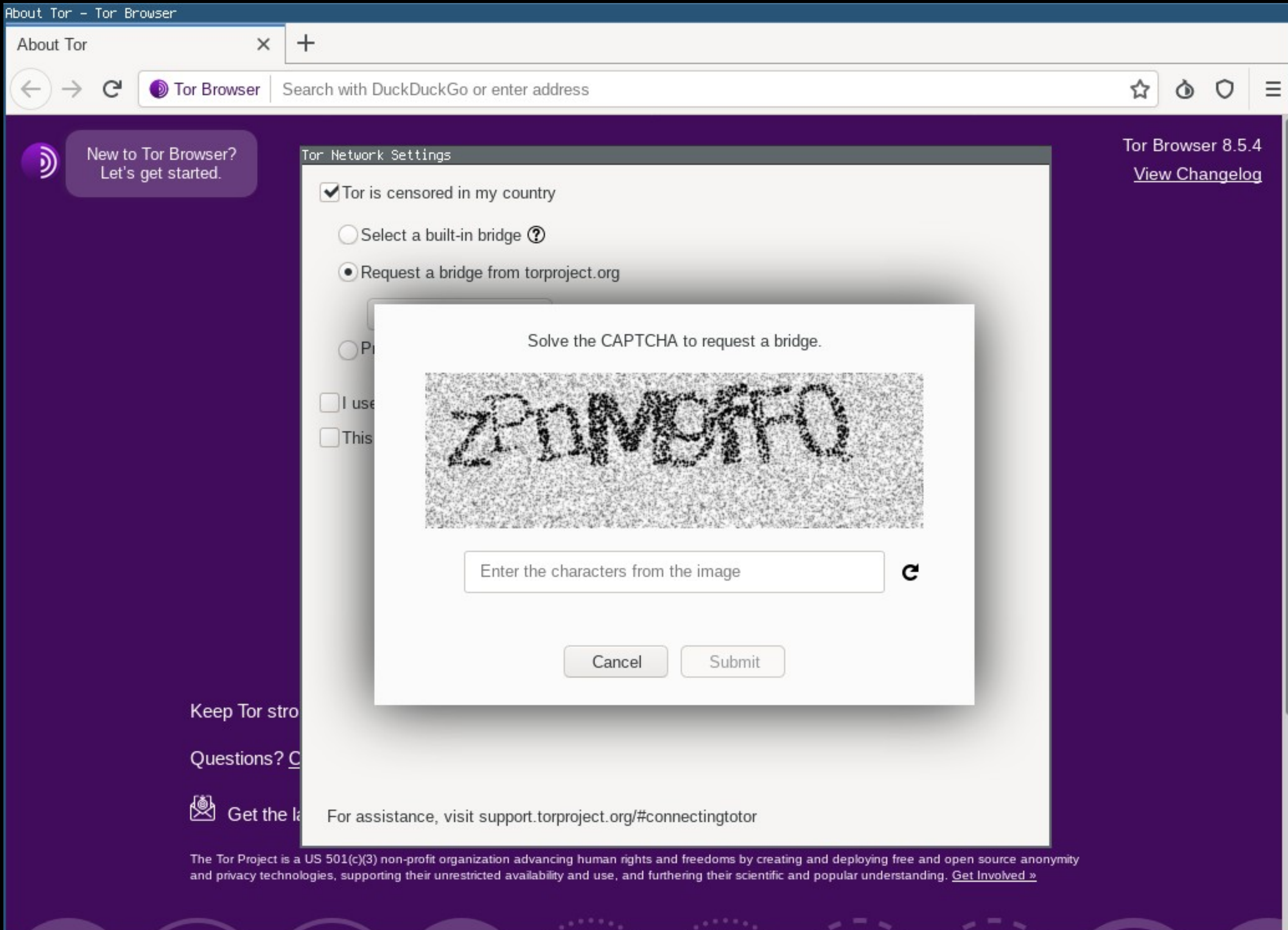
1) **https://bridges.torproject.org/** will tell you a few based on time and your IP address

2) Mail bridges@torproject.org from a gmail address and we'll send you a few

3) I mail some to a friend in Shanghai who distributes them via his social network

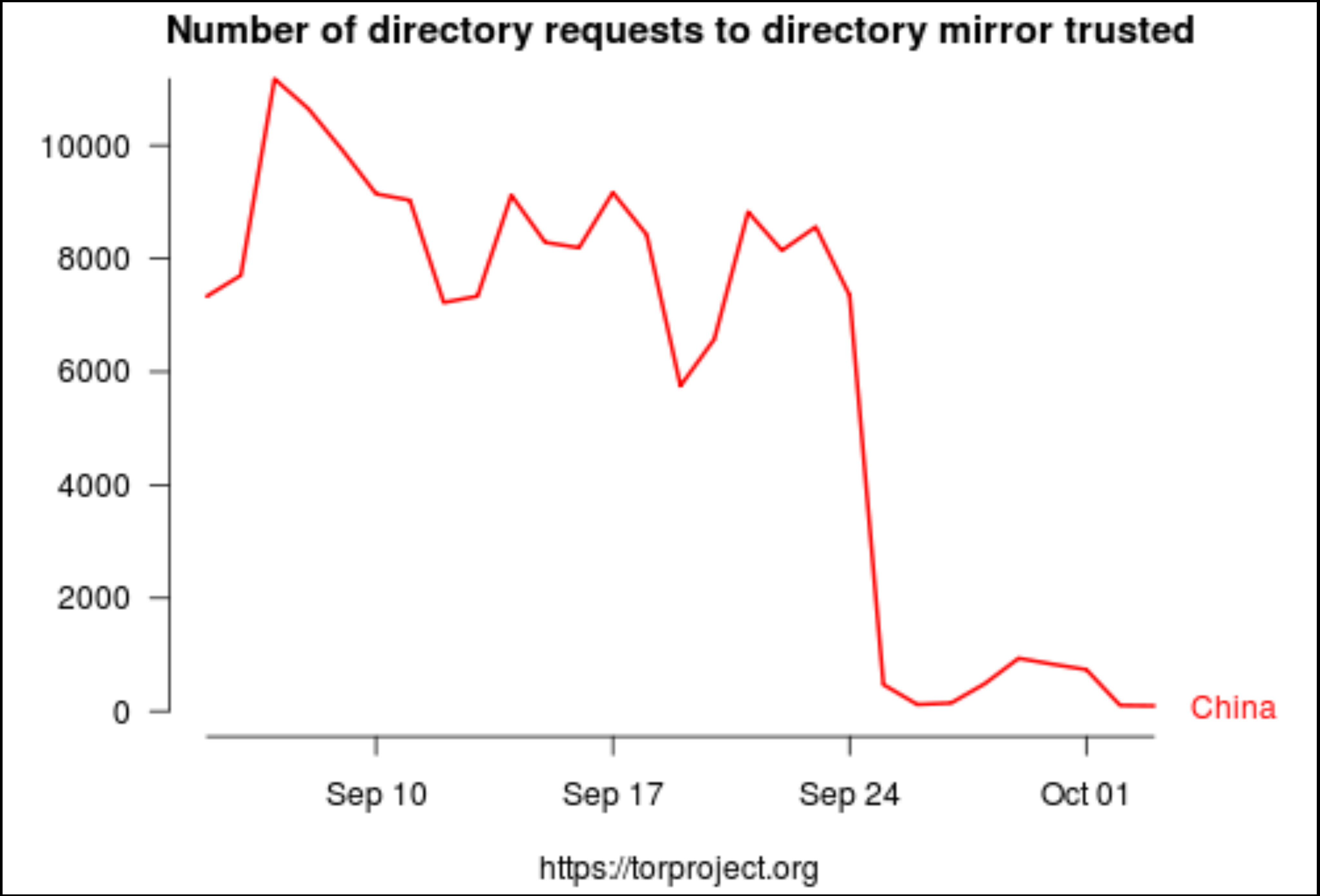
4) You can set up your own private bridge and tell your target users directly

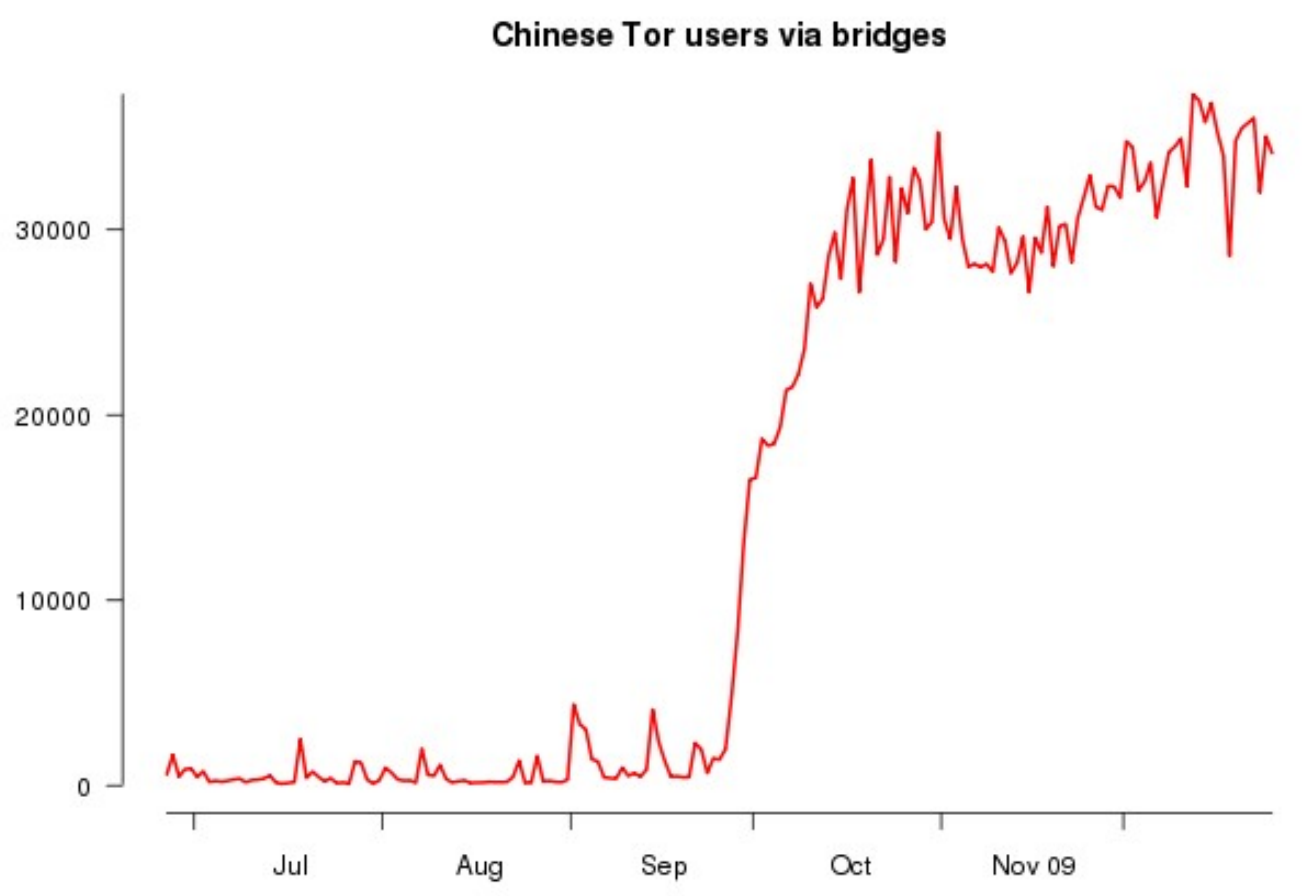

Tor Network Settings
Tor is censored in my country
Select a built-in bridge
Request a bridge from torproject.org
Provide a bridge I know
Enter bridge information from a trusted source.
type address:port (one per line)
I use a proxy to connect to the Internet
This computer goes through a firewall that only allows connections to certain ports


About Tor - Tor Browser
About Tor
Tor Browser
Search with DuckDuckGo or enter address
New to Tor Browser?
Let's get started.
Tor Network Settings
Tor is censored in my country
Select a built-in bridge
Request a bridge from torproject.org
Solve the CAPTCHA to request a bridge.
Enter the characters from the image
Cancel
Submit
For assistance, visit support.torproject.org/#connectingtotor
Tor Browser 8.5.4
View Changelog
Keep Tor stro
Questions? C
Get the l
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

China (September 2009)

- China grabbed the list of public relays and blocked them
- They also enumerated+blocked one of the three bridge buckets (https://bridges.torproject.org/)
- But they missed the other bridge buckets.


Number of directory requests to directory mirror trusted
10000
8000
6000
4000
2000
0
China
Sep 10
Sep 17
Sep 24
Oct 01
https://torproject.org

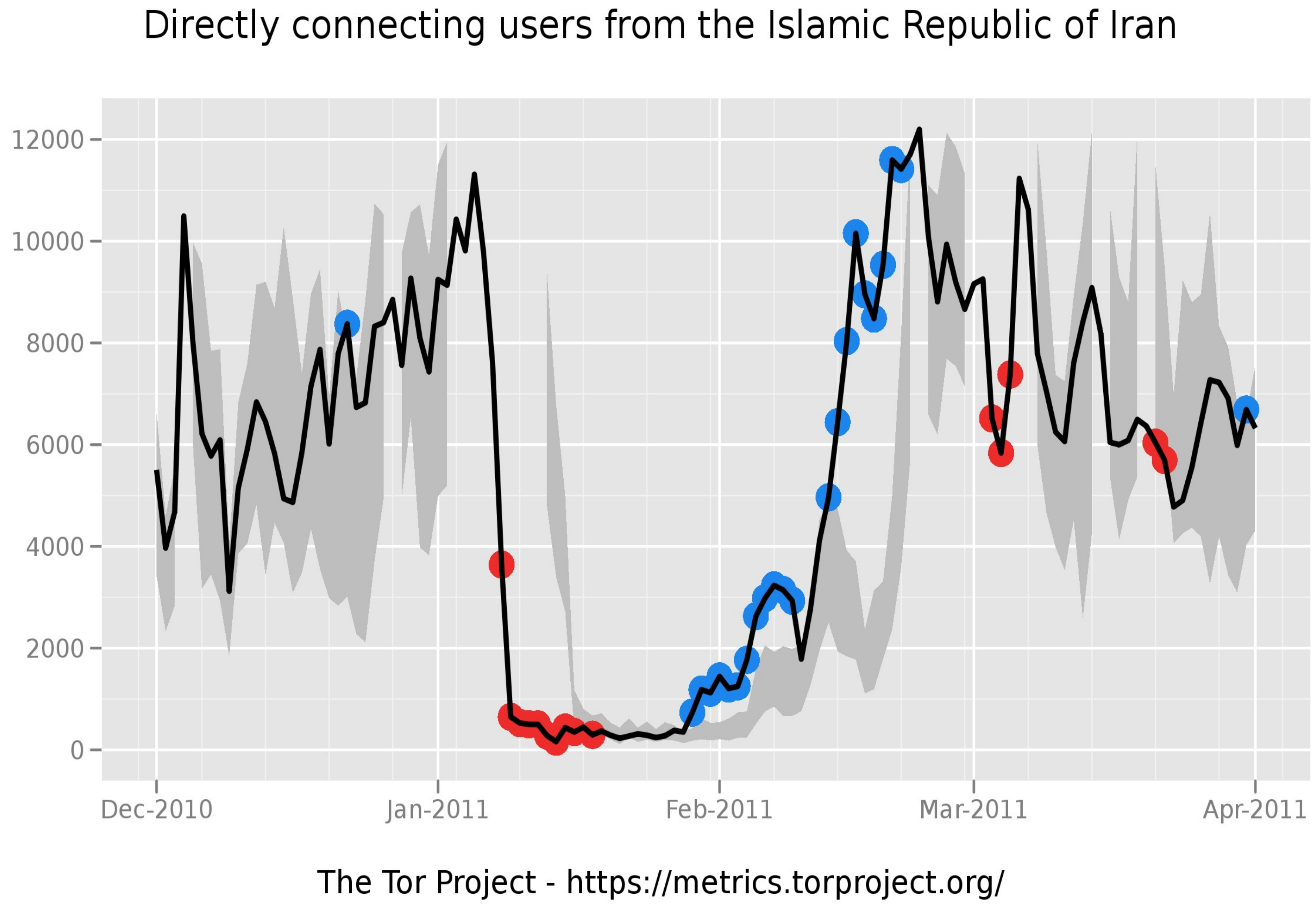

Chinese Tor users via bridges
30000
20000
10000
0
Jul
Aug
Sep
Oct
Nov 09

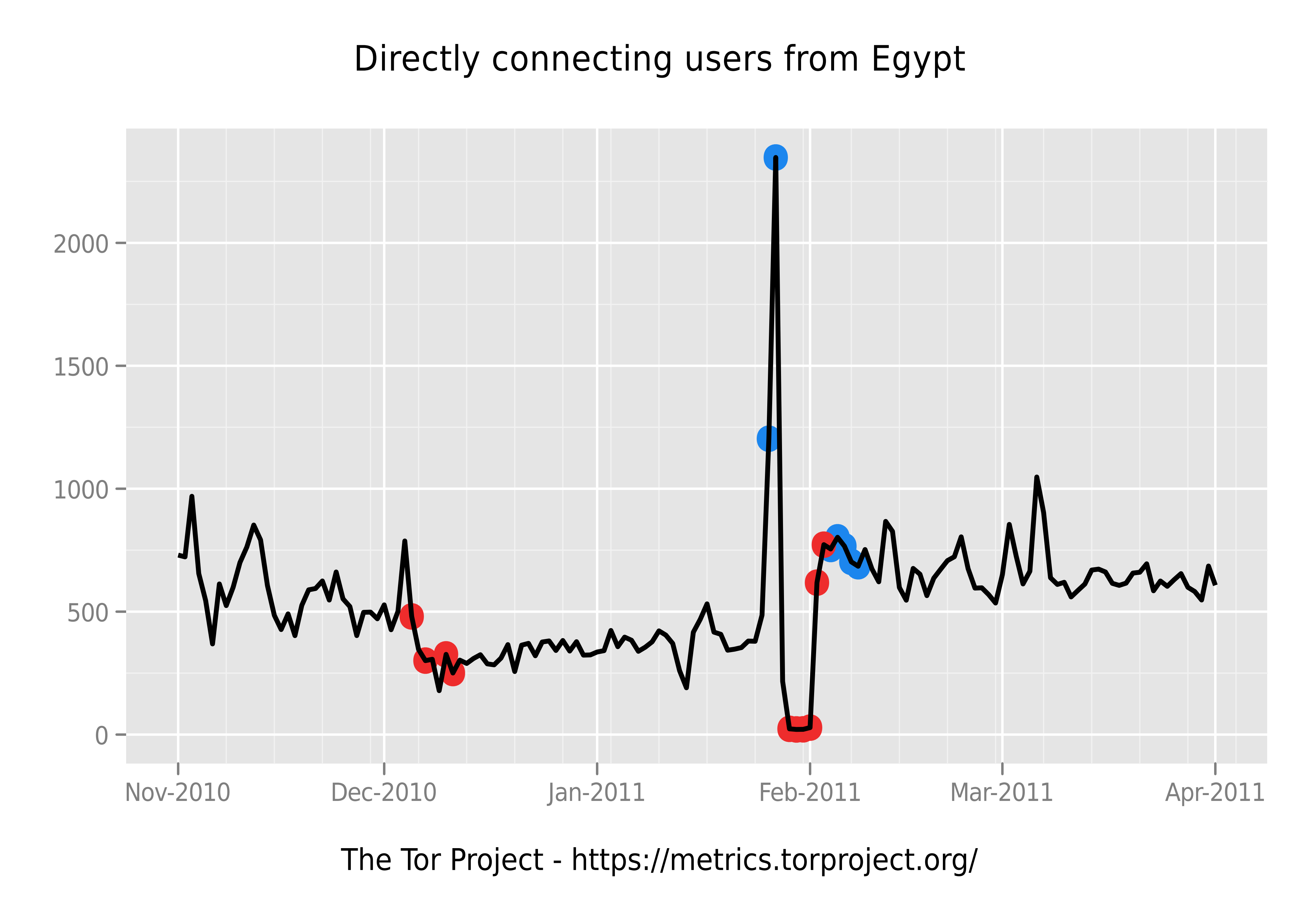
China (March 2010)

- China enumerated the second of our three bridge buckets (the ones available at bridges@torproject.org via Gmail)
- We were down to the social network distribution strategy, and the private bridges

Iran (January 2011)

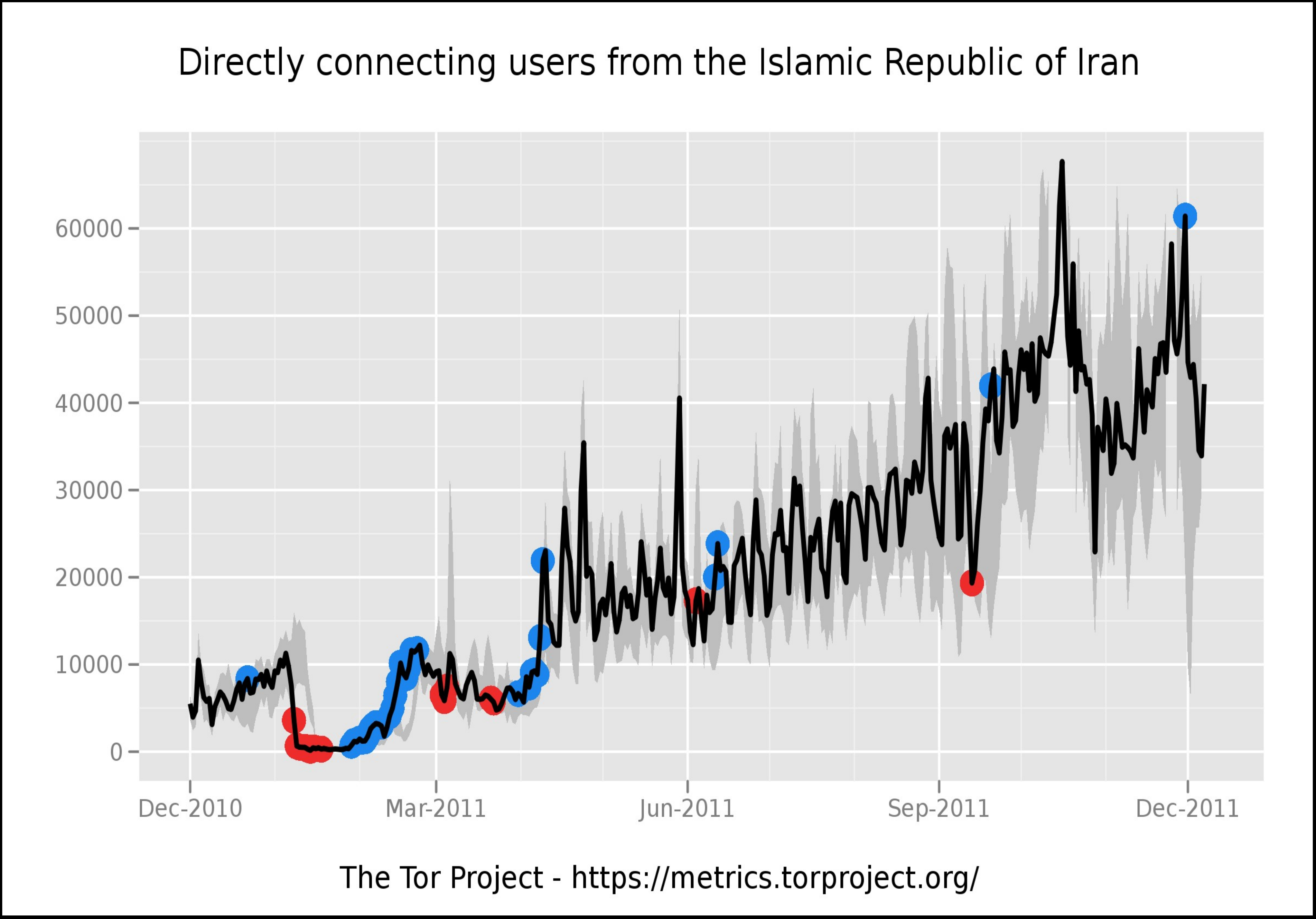
- Iran blocked Tor by DPI for SSL and filtering our Diffie-Hellman parameter.
- Socks proxy worked fine the whole time (the DPI didn't pick it up)
- DH p is a server-side parameter, so the relays and bridges had to upgrade, but not the clients


Directly connecting users from the Islamic Republic of Iran
12000
10000
8000
6000
4000
2000
0
Dec-2010
Jan-2011
Feb-2011
Mar-2011
Apr-2011
The Tor Project - https://metrics.torproject.org/


Directly connecting users from Egypt
2000
1500
1000
500
0
Nov-2010
Dec-2010
Jan-2011
Feb-2011
Mar-2011
Apr-2011
The Tor Project - https://metrics.torproject.org/

Iran (September 2011)

- This time, DPI for SSL and look at our TLS certificate lifetime.
- (Tor rotated its TLS certificates every 2 hours, because key rotation is good, right?)
- Now our certificates last for a year
- These are all low-hanging fruit. Kind of a weird arms race.


Directly connecting users from the Islamic Republic of Iran
60000
50000
40000
30000
20000
10000
0
Dec-2010
Mar-2011
Jun-2011
Sep-2011
Dec-2011
The Tor Project - https://metrics.torproject.org/

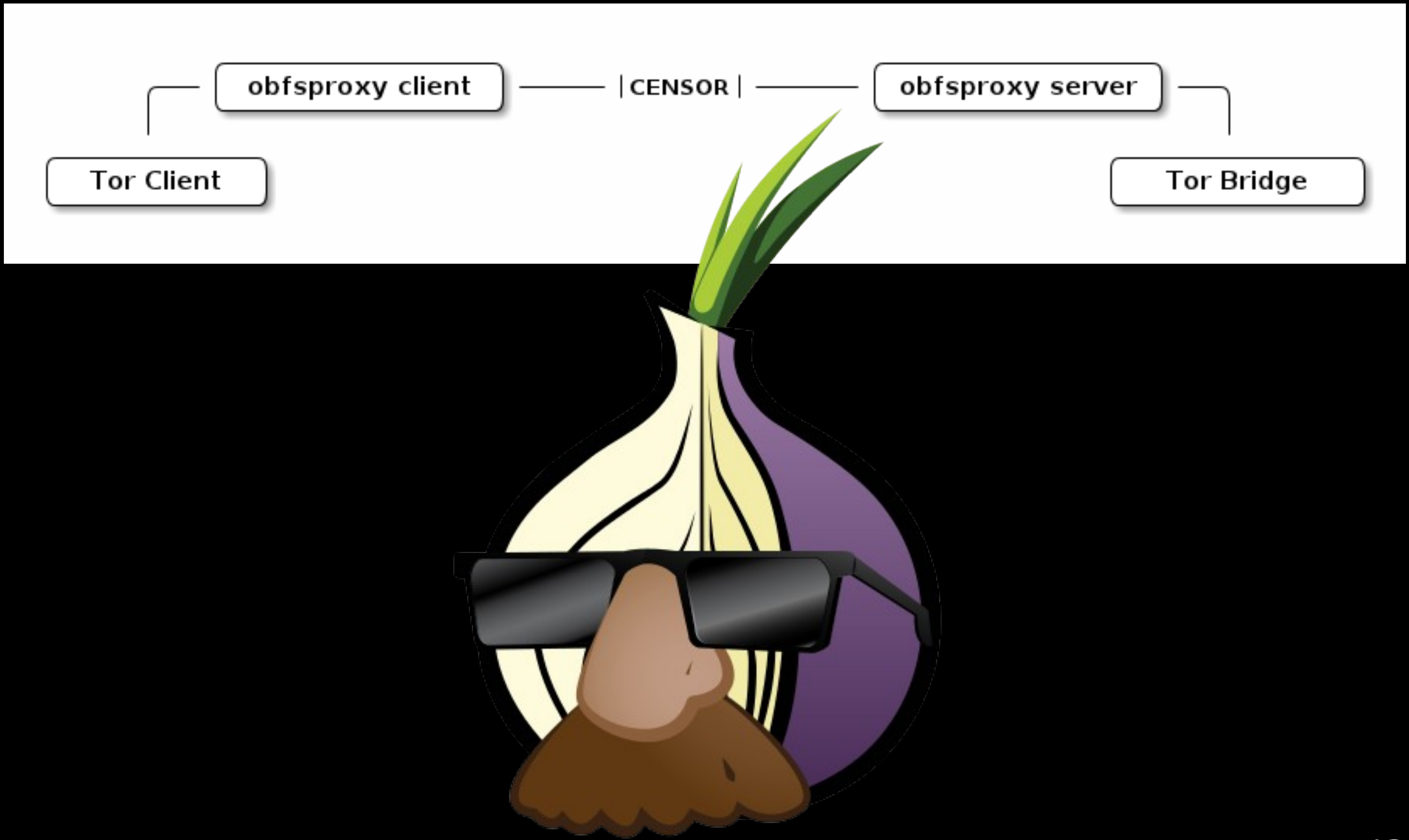

MESS WITH ONE OF US.
MESS WITH ALL OF US.
Supporting totalitarian regimes is our business.
Sleep safe Assad, Blue Coat is here.
Blue Coat


Auswärtiges Amt
Werderscher Markt 1
POLIZEI

Tunisia (October 2011)

- First country to announce officially that they censor
- Using Smartfilter
- Outsourced to a foreign corporation
- And Tunisia got a discount!

Pluggable transports



The two currently successful PTs

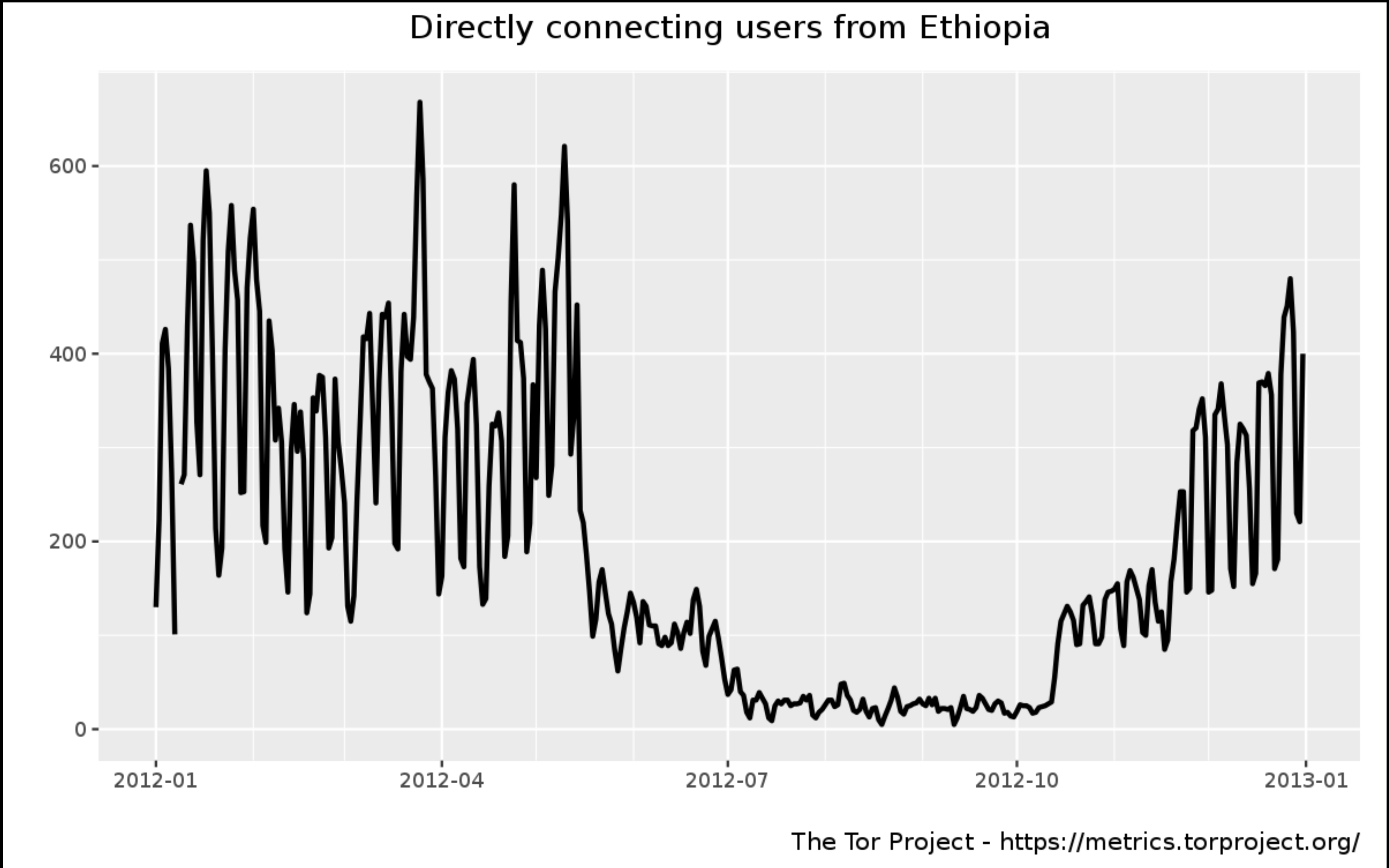
- obfsproxy (2012): add a layer of encryption on top so there are no recognizable headers.
- meek (2014): “domain fronting” via Google, Azure, Amazon

Tor censorship epochs

- ~~Background / Phase 1 (2006-2011):~~
  ~~Bridges, pluggable transports~~
- Phase 2 (2011-2019):
  Active probing, obfsproxy, domain fronting, many more countries
- Phase 3 (2019-?):
  Snowflake, obfs4, decoy routing, ...

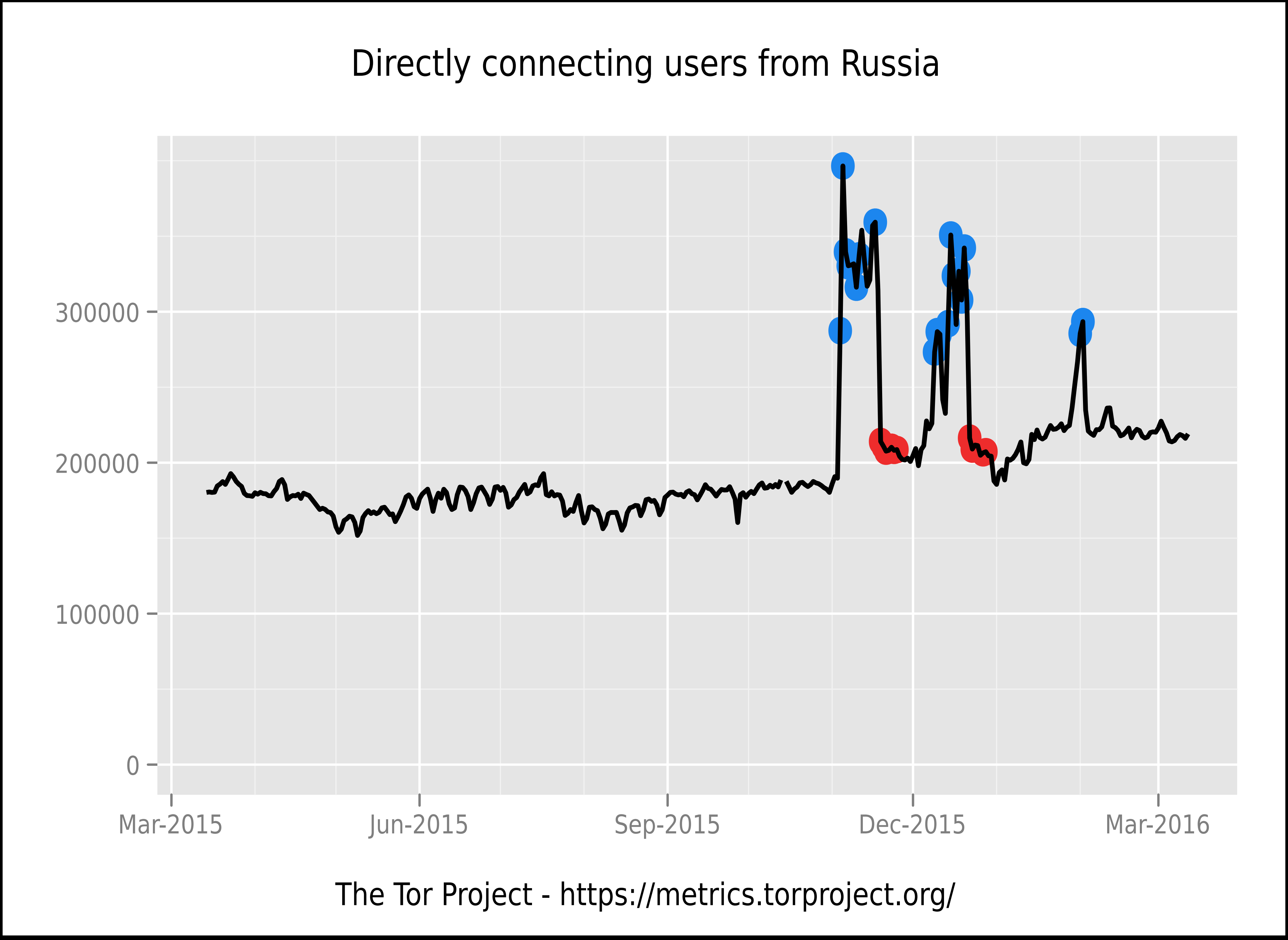
China (October 2011)

- Started its active probing campaign by DPIing on Tor’s TLS handshake, and later on obfs2 and obfs3
- Spoofed IP addresses from inside China
- The fix: obfs4 requires the client to prove knowledge of a secret, else it won’t admit to being an obfs4 bridge.

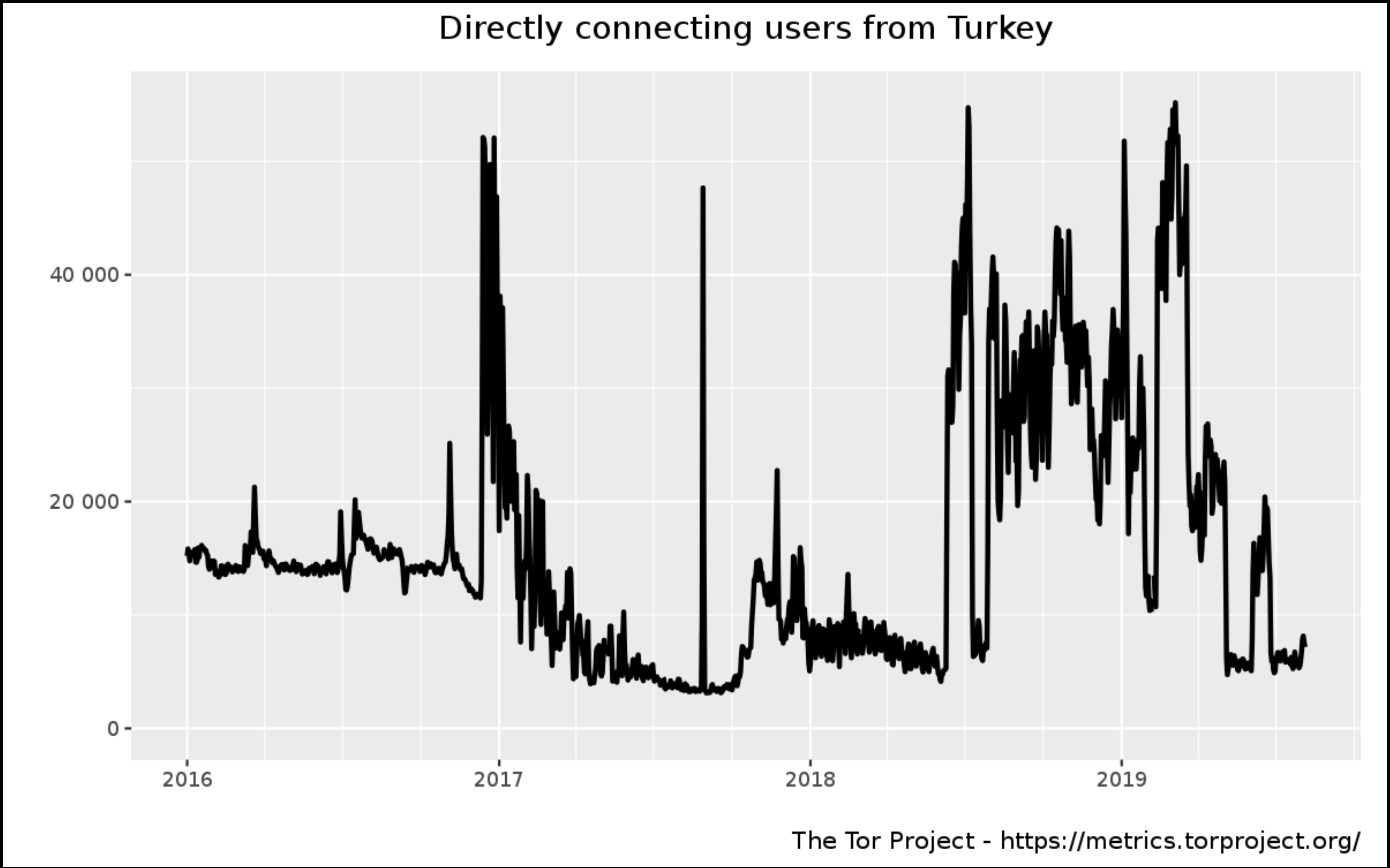

Directly connecting users from Ethiopia
600
400
200
0
2012-01
2012-04
2012-07
2012-10
2013-01
The Tor Project - https://metrics.torproject.org/

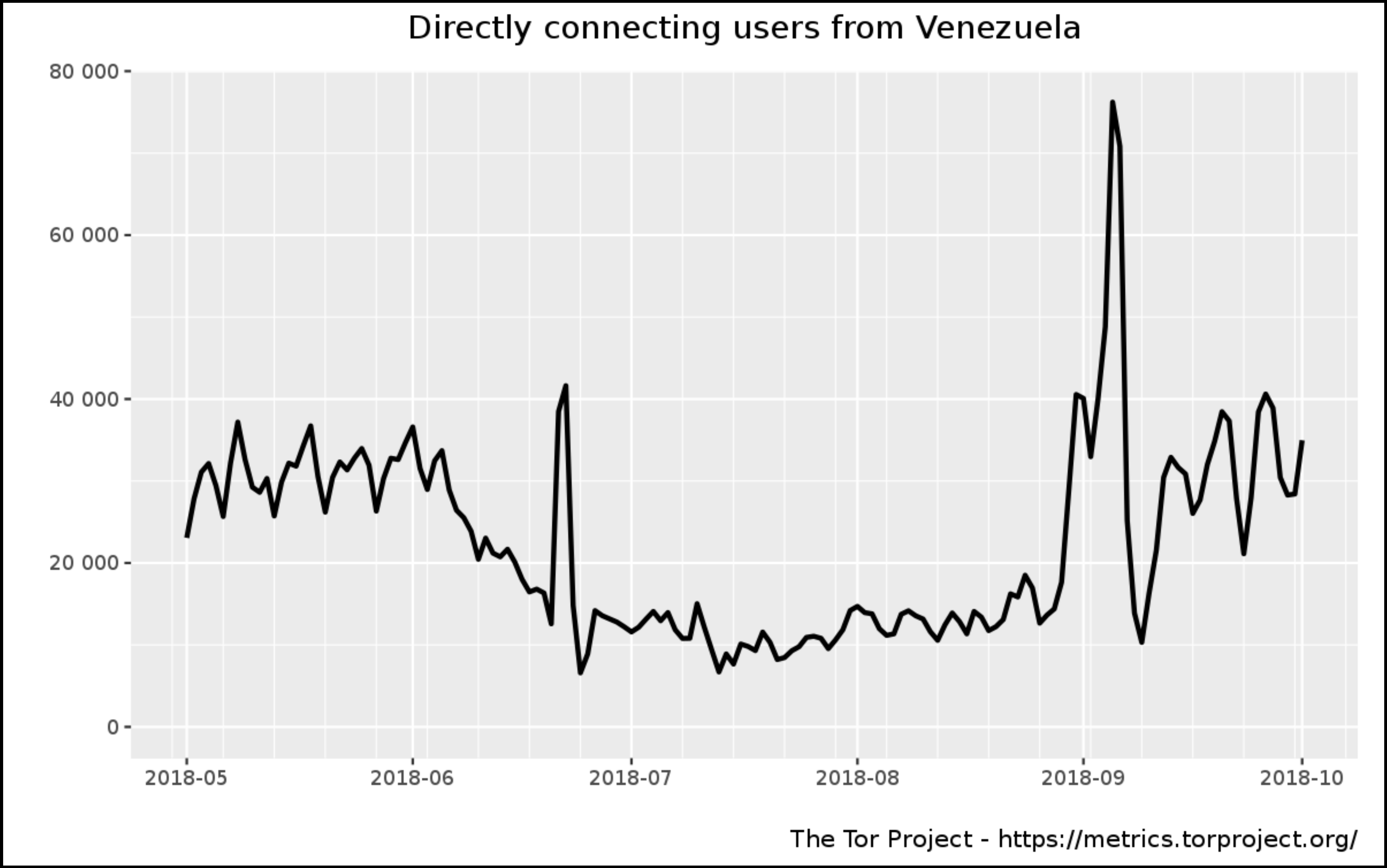
China (March 2015)

- “Great Cannon” targets github
- Greatfire declaring war, “you can’t block us”
- Huge difference from previous “let them save face” approach



Directly connecting users from Russia
300000
200000
100000
0
Mar-2015
Jun-2015
Sep-2015
Dec-2015
Mar-2016
The Tor Project - https://metrics.torproject.org/


Directly connecting users from Turkey
40 000
20 000
0
2016
2017
2018
2019
The Tor Project - https://metrics.torproject.org/


Directly connecting users from Venezuela
80 000
60 000
40 000
20 000
0
2018-05
2018-06
2018-07
2018-08
2018-09
2018-10
The Tor Project - https://metrics.torproject.org/

China (pre 2018)

- China also shifted to blackholing the entire IP address (not just the offending port).
- **<u>Any</u>** old probers are enough to get bridges blocked (0.2.9, ORPort, etc)

China (mid 2018)

- Lantern uses obfs4 proxies for its own circumvention tool
- After a while, the proxies they give their users don’t work so well.

^ another example of tough feedback loop

China (mid 2019)

- 0.3.2 Tor clients, talking to 0.3.5 Tor bridges, don’t trigger active probing anymore.
- We guess it has to do with changes in advertised ciphersuites on the client side.

Technology Intelligence

Dozens of US spies killed after Iran and China uncovered CIA messaging service using Google




I CAN HAZ
FREEDOM?
Tor
TorProject.org




East-Turkestan
(XinJiang)
CHINA

Tor censorship epochs

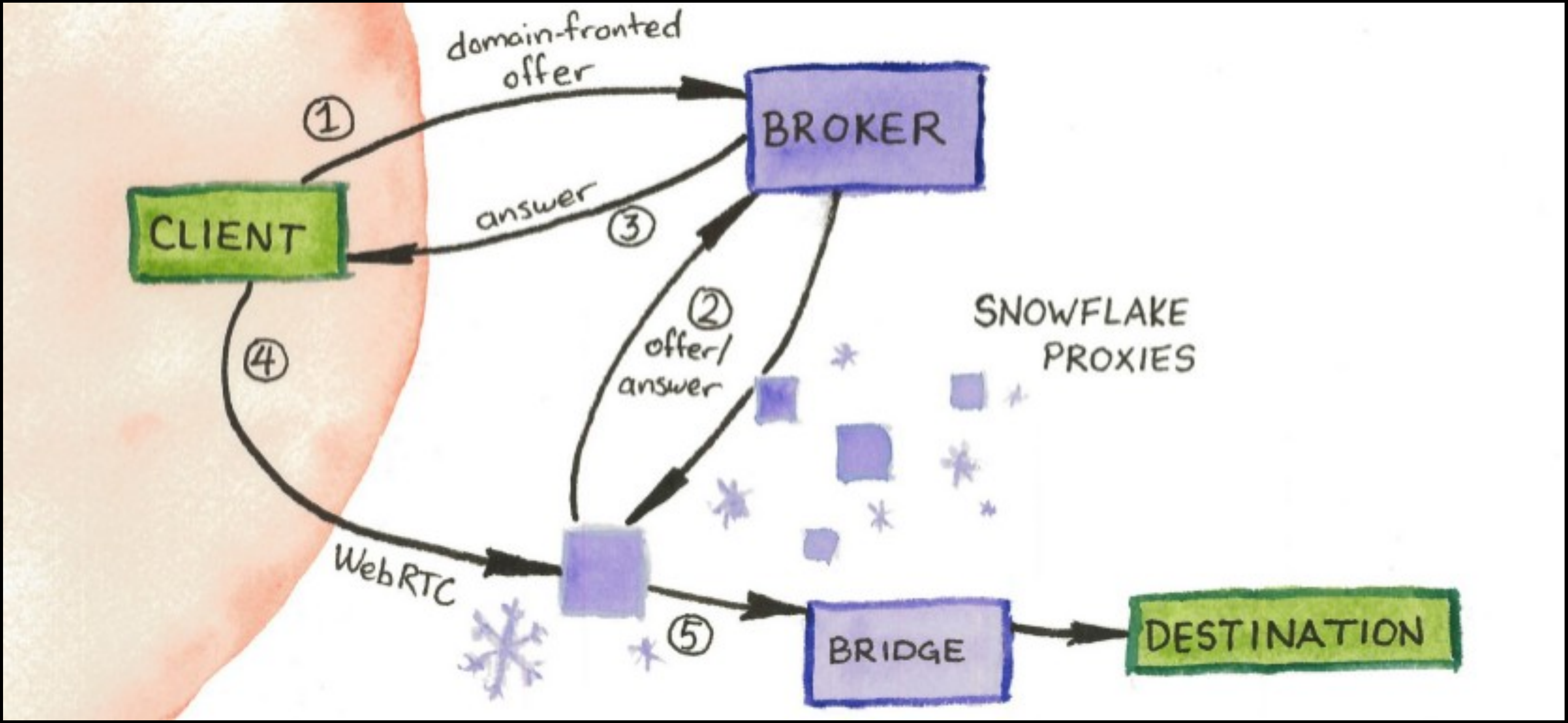
- ~~Background / Phase 1 (2006-2011):~~

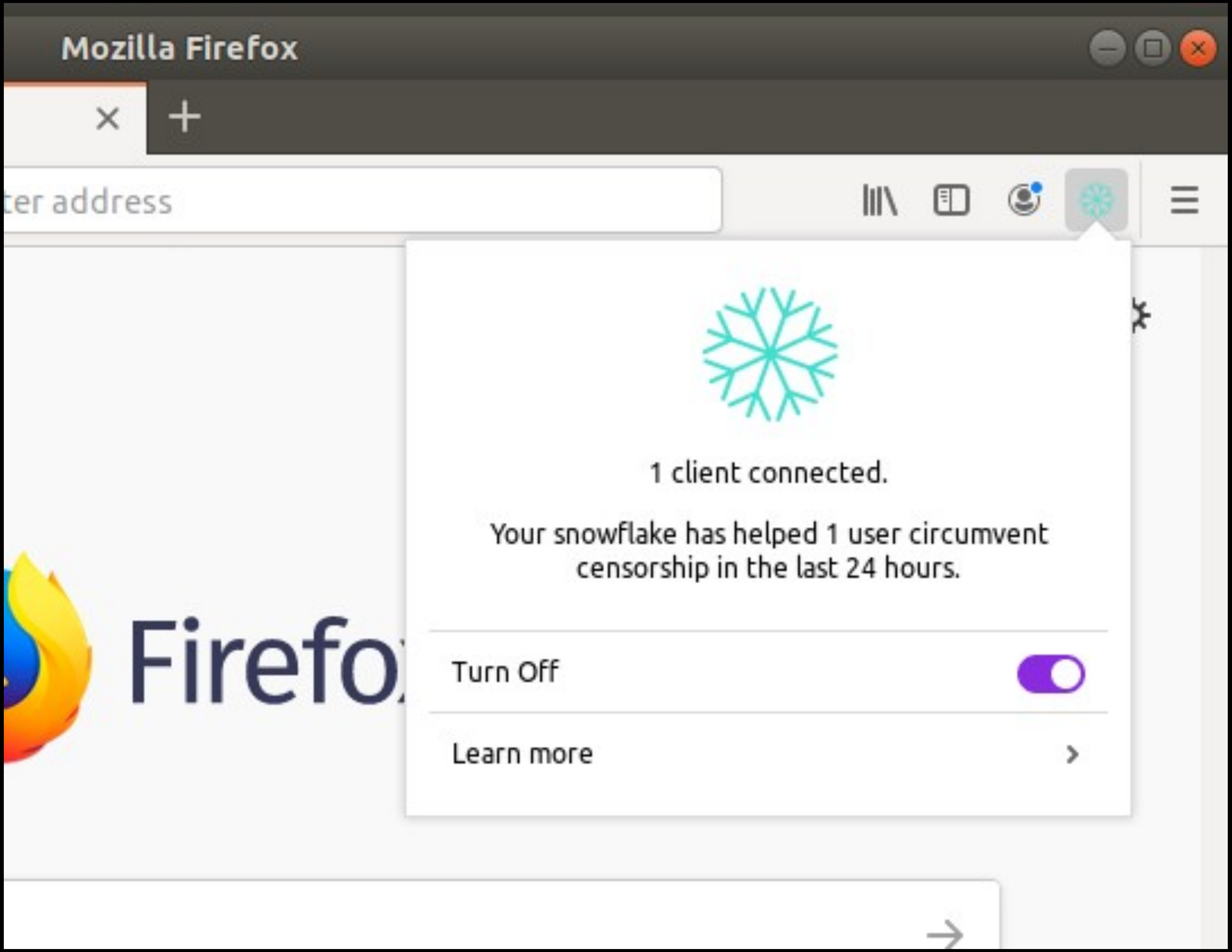
  ~~Bridges, pluggable transports~~
- ~~Phase 2 (2011-2019):~~

  ~~Active probing, obfsproxy, domain fronting, many more countries~~
- Phase 3 (2019-?):

  Snowflake, obfs4, decoy routing, ...

New pluggable transport: Snowflake




Mozilla Firefox
ter address
1 client connected.
Your snowflake has helped 1 user circumvent censorship in the last 24 hours.
Turn Off
Learn more
Firefo



What do the icons mean?

Working: if your status is light blue or dark blue, your proxy is running.

 A plain pink cupcake means the proxy is running but no one is using it right now.

 A happy cupcake means someone is using your proxy right now. Neat!

Not working: if your status is grey or black, there was a problem and your proxy is not running. Usually this is due to internet connection problems or firewall settings.

 A sad grey cupcake means that the badge has disabled itself. Try restarting your browser.

Streamlined obfs4 deployment

- https://community.torproject.org/relay/setup/bridge
- The future: “apt install tor-servers” ?

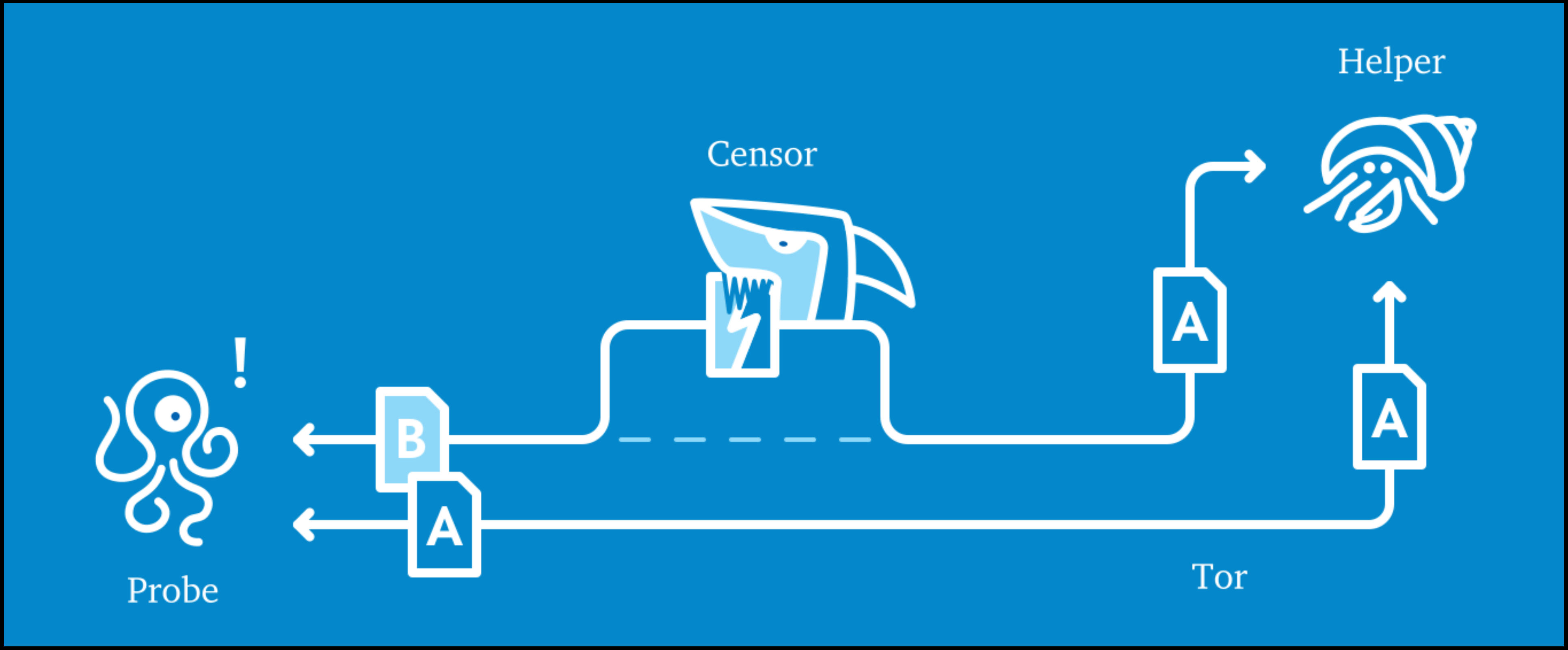
BridgeDB needs a feedback cycle

- Measure how much use each bridge sees
- Measure bridge blocking
- Then adapt bridge distribution to favor efficient distribution channels
- Need to invent new distribution channels, eg Salmon from PETS 2015

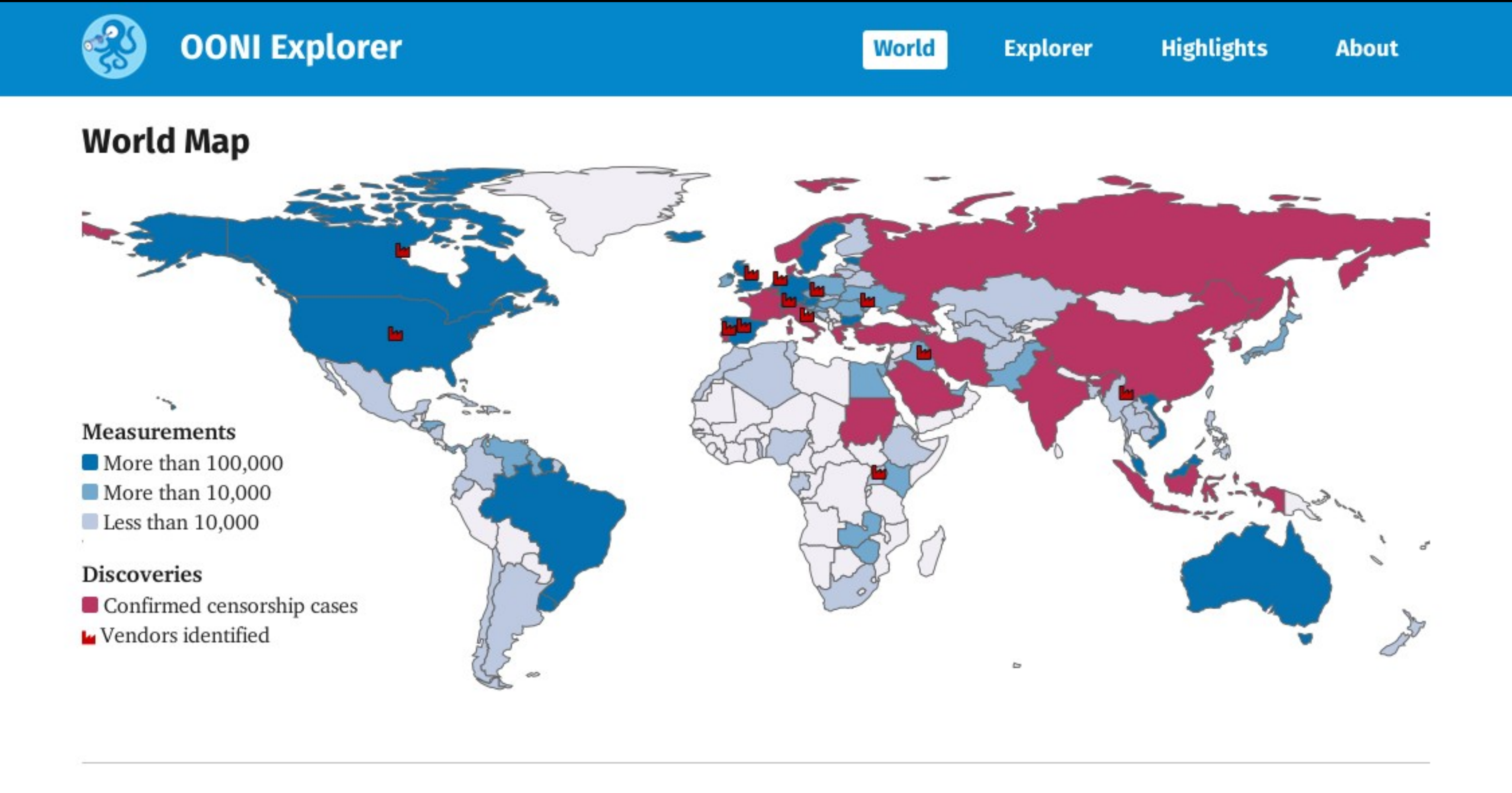
Measuring bridge reachability

- Passive: bridges track incoming connections by country; clients self-report blockage (via some other bridge)
- Active: scan bridges from within the country; or measure remotely via indirect scanning
- Bridges test for duplex blocking

ooni.torproject.org



explorer.ooni.torproject.org



Other upcoming designs

- FTE/Marionette: transform traffic payloads according to a regexp or a state machine
- Decoy routing: run a tap at an ISP, look for steganographic tags, inject responses from the middle

Arms races

- Censorship arms race is bad
- Surveillance arms race is worse
  - And centralization of the Internet makes it worse still

How can you help?

- Run an obfs4 bridge, be a Snowflake
- Teach your friends about Tor, and privacy in general
- Help find – and fix – bugs
- Work on open research problems (petsymposium.org)
- donate.torproject.org

TOR'S BUG SMASH FUND

donate.torproject.org


3V3
GND



TorProject.org
anonymity online
torproject.org
Tor
We believe everyone should have private access to the open web.
MISSION
The Tor Project, Inc., is a 501(c)(3) organization headquartered in Seattle with paid staff and contractors of around 35 engineers and operational support people, plus many volunteers all over the world. Tor develops free and open source software for privacy and freedom online, protecting people from tracking, surveillance, and censorship. The Tor Project's mission is to advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, support their unrestricted availability and use, and further their scientific and popular understanding.
THE TOR NETWORK
The Tor network is a decentralized network of volunteer run servers around the world.
Before reaching the website you're visiting, your traffic is encrypted three times as it passes over these servers.
HOW TOR WORKS
Alice encrypts her web page request to Bob three times and sends it to the first relay.
The first relay removes the first encryption layer but doesn't learn that the web page request goes to Bob.
The second relay removes another encryption layer and forwards the web page request.
The third relay removes the last encryption layer and forwards the web page request to Bob, but doesn't know that it comes from Alice.
Bob doesn't know that the web page request came from Alice, unless she tells him so.